CD820 & (I)FD820 Series

HD Fixed Dome Network Cameras

User Manual

Note: To ensure proper operation, please read this manual thoroughly before using the product and retain the information for future reference.

Copyright © 2014 Siqura B.V.

All rights reserved.

CD/(I)FD820
User Manual v4 (122002-4)
AIT55

Nothing from this publication may be copied, translated, reproduced, and/or published by means of printing, photocopying, or by any other means without the prior written permission of Siqura.

Siqura reserves the right to modify specifications stated in this manual.

Brand names

Any brand names mentioned in this manual are registered trademarks of their respective owners.

Liability

Siqura accepts no liability for claims from third parties arising from improper use other than that stated in this manual.

Although considerable care has been taken to ensure a correct and suitably comprehensive description of all relevant product components, this manual may nonetheless contain errors and inaccuracies. We invite you to offer your suggestions and comments by email via t.writing@tkhsecurity.com. Your feedback will help us to further improve our documentation.

How to contact us

If you have any comments or queries concerning any aspect related to the product, do not hesitate to contact:

Siqura B.V.
Zuidelijk Halfrond 4
2801 DD Gouda
The Netherlands

General : +31 182 592 333
Fax : +31 182 592 123
E-mail : sales.nl@tkhsecurity.com
WWW : www.siqura.com

Contents

1 About this manual 6

2 Safety and compliance 7

2.1 Safety 7
2.2 Cautions 9
2.3 Compliance 10

3 Product overview 11

3.1 Models 11
3.2 Description 13

4 Access the webpages 14

4.1 System requirements 14
4.2 Connect via web browser 14
4.3 Find the unit with Siqura Device Manager 15
4.4 Change the network settings with Siqura Device Manager 16
4.5 Log on to the unit 17
4.6 Install Siqura Viewer 18
4.7 The CD/(I)FD820 Web Interface 18

5 Home 20

5.1 CD820/IFD820 20
5.2 FD820 21
5.3 Home page functions 22
5.4 Zoom and focus (FD820) 23

6 System settings 24

6.1 System 25
6.1.1 Host name 25
6.1.2 Time zone 25
6.1.3 Daylight saving time 25
6.1.4 Time format 26
6.1.5 Time synchronisation 26
6.2 Security 26
6.2.1 User 27
6.2.1.1 Admin password 27
6.2.1.2 Add and manage user accounts 27
6.2.1.3 Streaming Authentication Setting 28
6.2.2 HTTPS 29
6.2.2.1 Create a self-signed certificate 30
6.2.2.2 Create and install a signed certificate 30
6.2.3 IP filter 31
6.2.4 IEEE 802.1X 32
6.2.4.1 CA certificate 32
6.2.4.2 Client certificate and private key 32
6.3 Network 33
6.3.1 Basic 33
6.3.1.1 Acquire an IP address automatically 33
6.3.1.2 Modify the fixed IP address 34
6.3.1.3 Use PPPoE 35
6.3.1.4 Advanced settings 35
6.3.1.5 IPv6 address configuration 35

6.3.2 QoS 36
6.3.3 SNMP 37
6.3.4 UPnP 39
6.4 DDNS 40
6.5 Mail 41
6.6 FTP 42
6.7 HTTP 43
6.8 Events 43
6.8.1 Application 44
6.8.1.1 Triggered action 45
6.8.1.2 Specifying file name conventions 47
6.8.2 Motion detection 48
6.8.2.1 Motion detection area 49
6.8.2.2 Motion detection window 50
6.8.3 Network failure detection 51
6.8.4 Tampering 52
6.8.5 Periodical event 53
6.8.6 Manual trigger 54
6.8.7 Audio detection 55
6.9 Storage management 56
6.9.1 SD Card 56
6.9.2 Network Share 58
6.10 Recording 60
6.11 Schedule 61
6.12 File location 62
6.13 View information 62
6.13.1 Log file 63
6.13.2 User Information 64
6.13.3 Parameters 65
6.14 Factory default 66
6.15 Software version 67
6.16 Software upgrade 67
6.17 Maintenance 68

7 Streaming 70
7.1 Video format 70
7.1.1 Video resolution 71
7.1.2 Video rotate type 71
7.1.3 GOV Settings 71
7.1.4 H.264 Profile 71
7.2 Video compression 72
7.3 Video ROI 73
7.4 Video text overlay 74
7.5 Video stream protocol 75
7.6 Video frame rate 76
7.7 Video mask 77
7.8 Audio 78

8 Camera 80
8.1 Exposure 80
8.1.1 Auto mode 81
8.1.2 Manual mode 81
8.2 White Balance 82
8.3 Picture Adjustment 83
8.4 Backlight 84
8.5 Digital Zoom 84

8.6 IR Function (FD820 & IFD820) 84
8.7 WDR Function 85
8.8 Noise Reduction 85
8.9 Profile 86
8.10 TV System 87

Appendix: Enable UPnP components in Windows 7 88

Appendix: Delete the existing Siqura Viewer software 89

Appendix: Set up Internet security 90

Index 91

1 About this manual

What this manual covers

This manual applies to the (I)FD820 and CD820 series, Siqura's HD fixed dome and compact fixed dome network cameras.

Note: In this manual, "CD/(I)FD820" is the product name used when describing features common to all (I)FD820 and CD820 models. In descriptions of distinguishing features, the relevant model name is used.

This manual explains:

- How to access the camera
- How to communicate with the camera
- How to operate the camera
- How to configure the camera's settings

For instructions on camera installation and establishing connections, see the separate Quick Start Guide and Installation Manual supplied with each CD/(I)FD820 series model.

Who should read this manual

This manual is intended for technicians and operators involved in the configuration and operation of CD/(I)FD820 cameras.

What you should already know

To work with a CD/(I)FD820, a technician or operator should have adequate knowledge and skills in the fields of:

- Ethernet network technologies and Internet Protocol (IP)
- Windows environments
- Web browsers
- Video, audio, data, and contact closure transmissions
- Video compression methods

Before you proceed

Before you proceed, please read and observe all instructions and warnings in this manual. Retain this manual with the original bill of sale for future reference and, if necessary, warranty service. When unpacking your product, check for missing or damaged items. If any item is missing, or if damage is evident, do not install or operate this product. Contact your supplier for assistance.

Why specifications may change

At Siqura, we are committed to delivering high-quality products and services. The information given in this manual was current when published. As we are relentlessly working to improve our products and user experience, all specifications are subject to change without notice.

We like to hear from you!

Customer satisfaction is our first priority. We welcome and value your opinion about our products and services. Should you detect errors or inaccuracies in this manual, we would be grateful if you would inform us. We invite you to offer your suggestions and comments via t.writing@tkhsecurity.com. Your feedback helps us to further improve our documentation.

2 Safety and compliance

This chapter presents the CD/(I)FD820 safety instructions and compliance information.

In This Chapter

2.1 Safety....7
2.2 Cautions....9
2.3 Compliance....10

2.1 Safety

The safety information contained in this section, and on other pages of this manual, must be observed whenever this unit is operated, serviced, or repaired. Failure to comply with any precaution, warning, or instruction noted in the manual is in violation of the standards of design, manufacture, and intended use of the module. Siqura assumes no liability for the customer's failure to comply with any of these safety requirements.

Trained personnel

Installation, adjustment, maintenance, and repair of this equipment are to be performed by trained personnel aware of the hazards involved. For correct and safe use of the equipment and in order to keep the equipment in a safe condition, it is essential that both operating and servicing personnel follow standard safety procedures in addition to the safety precautions and warnings specified in this manual, and that this unit be installed in locations accessible to trained service personnel only.

Safety requirements

The equipment described in this manual has been designed and tested according to the **UL/IEC/EN 60950-1** safety requirements. See the CE Declaration of Conformity for compliance information.

Warning: If there is any doubt regarding the safety of the equipment, do not put it into operation.

This might be the case when the equipment shows physical damage or is stressed beyond tolerable limits (for example, during storage and transportation).

Important: Before opening the equipment, disconnect it from all power sources.

The equipment must be powered by a SELV[1] power supply. This is equivalent to a Limited Power source (LPS, see UL/IEC/EN 60950-1 clause 2.5) or a "NEC Class 2" power supply. When this module is operated in extremely elevated temperature conditions, it is possible for internal and external metal surfaces to become extremely hot.

1. SELV: conforming to IEC 60950-1, <60 Vdc output, output voltage galvanically isolated from mains. All power supplies or power supply cabinets available from Siqura comply with these SELV requirements.

Power source and temperature ratings

Verify that the power source is appropriate before you plug in and operate the unit. Use the unit under conditions where the temperature remains within the range given in the Technical Specifications of this product.

Optical safety

The following optical safety information applies to CD/(I)FD820 models with SFP interface.

This product complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007. This optical equipment contains Class 1M lasers or LEDs and has been designed and tested to meet **IEC 60825-1:1993+A1+A2** and **IEC 60825-2:2004 safety class 1M** requirements.

Warning: Optical equipment presents potential hazards to testing and servicing personnel, owing to high levels of optical radiation.

When using magnifying optical instruments, avoid looking directly into the output of an operating transmitter or into the end of a fiber connected to an operating transmitter, or there will be a risk of permanent eye damage. Precautions should be taken to prevent exposure to optical radiation when the unit is removed from its enclosure or when the fiber is disconnected from the unit. The optical radiation is invisible to the eye.

Use of controls or adjustments or procedures other than those specified herein may result in hazardous radiation exposure.

The installer is responsible for ensuring that the label depicted below (background: yellow; border and text: black) is present in the restricted locations where this equipment is installed.

EMC

This device has been tested and found to meet the CE regulations relating to EMC and complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. These limits are designed to provide reasonable protection against interference to radio communications in any installation. The equipment generates, uses, and can radiate radio frequency energy; improper use or special circumstances may cause interference to other equipment or a performance decrease due to interference radiated by other equipment. In such cases, the user will have to take appropriate measures to reduce such interactions between this and other equipment.

Any interruption of the shielding inside or outside the equipment could make the equipment more prone to fail EMC requirements.

Non-video signal lines must use appropriate shielded Cat 5 cabling (S-FTP), or at least an equivalent. Ensure that *all* electrically connected components are carefully earthed and protected against surges (high voltage transients caused by switching or lightning).

ESD

Electrostatic discharge (ESD) can damage or destroy electronic components. *Proper precautions should be taken against ESD when opening the equipment.*

RoHS statement

Global concerns over the health and environmental risks associated with the use of certain environmentally-sensitive materials in electronic products have led the European Union (EU) to enact the Directive on the Restriction of the use of certain Hazardous Substances (RoHS) (2002/95/EC). Siqura offers products that comply with the EU's RoHS Directive. The full version of the Siqura RoHS statement can be viewed at www.siqura.com.

Product disposal

The unit contains valuable materials which qualify for recycling. In the interest of protecting the natural environment, properly recycling the unit at the end of its service life is imperative.

When processing the printed circuit board, dismantling the lithium battery calls for special attention. This kind of battery, a button cell type, contains so little lithium, that it will never be classified as reactive hazardous waste. It is safe for normal disposal, as required for batteries by your local authority.

2.2 Cautions

Handle the camera carefully

Do not abuse the camera. Avoid bumping and shaking. The camera can be damaged by improper handling or storage.

Do not disassemble the camera

To prevent electric shock, do not remove screws or covers. There are no user serviceable parts inside. Consult technical support if a camera is suspected of malfunctioning.

Do not expose indoor models to moisture

The indoor camera is designed for indoor use or use in locations where it is protected from rain and moisture. Turn the power off immediately if the camera is wet and ask a qualified technician for servicing. Moisture can damage the camera and also create the danger of electric shock.

Do not use strong or abrasive detergents to clean the camera

Use a dry cloth to clean the camera when it is dirty. If the dirt is hard to remove, use a mild detergent and wipe gently. To clean the lens, use lens tissue or a cotton tipped applicator and ethanol. Do *not* clean the lens with strong detergents.

Never face the camera towards the sun

Do not aim the camera at bright objects. Whether the camera is in use or not, never aim it at the sun or other extremely bright objects, as this can damage the camera.

2.3 Compliance

CE

DECLARATION OF CONFORMITY

TKH GROUP | TKH SECURITY SOLUTIONS

Product identification

Product:	HD Surveillance Cameras (820 series) Network (IP) cameras, box, dome or PTZ
Brand:	Siqura
Model/type:	**BC820, BL820, CD820, ICD 820** series **FD820, IFD820** and **HSD820** series
Versions:	(a)820(b) (a) Replaced by one of these prefixes: BC, BL, CD, ICD, FD, IFD, HSD (b) May be followed by: any combination of characters, including -SFP
Ratings:	12VDC / 24VAC / PoE
Tested:	System is tested in a typical configuration, SFP version is tested by Siqura with Siqura ECO-plug Ethernet over Coax SFP.

SIQURA SURVEILLANCE SOLUTIONS

Means of conformity

In conformity with provisions of the following EC directives:
LVD: 2006/95/EC, EMC: 2004/108/EC.

A sample of the product has been evaluated by

LVD: (Safety)	Siqura B.V., Gouda, The Netherlands
Standards:	IEC 60950-1:2005, EN 60950-1:2006 Information Technology Equipment – Safety - Part 1: general requirements.
EMC:	Siqura B.V., Gouda, The Netherlands
Standards:	EN 55022:2006+A1 - Emission, Residential. (Class A) FCC 47 CFR 15 - Emission, Residential (Class A) EN 61000-3-2, EN 61000-3-3 EN 61000-6-2 – Generic, Immunity, Industrial EN 61000-series: Parts: 4-2, 4-3, 4-4, 4-5, 4-6, 4-11 EN 50130-4:1995+A1+A2 *exception: ECO-plug is tested according Railway standards EN 50121-3-2 (tested at 10V/m) and EN 50121-4

Company

Name:	Siqura B.V.	TKH Security Solutions USA, Inc.
Address:	Zuidelijk Halfrond 4 2801 DD Gouda, The Netherlands www.siqura.com	12920 Cloverleaf Center Drive Germantown, MD 20874, USA www.tkhsecurity.com

Signature

Name:	M.H.M. Perquin	W.D. Hermelink
Title:	Director Customer Services	Product Certification Engineer
Date:	Gouda, 2014 October 15	

3 Product overview

CD/(I)FD820 series cameras are HD fixed dome network cameras providing high-quality high-definition images. This chapter introduces the individual models and their features.

In This Chapter

3.1 Models.....11

3.2 Description.....13

3.1 Models

CD820F1

HD Compact fixed dome IP camera

- Multiple resolutions: 1080p/720p
- 1/2.7” Progressive scan CMOS imager
- Quad-stream H.264 and MJPEG video
- ONVIF compliant
- Audio - mic input
- 3.6 mm fixed lens
- Compact surface mount design
- Ruggedised construction
- 802.3af Power-over-Ethernet / 12 Vdc
- IP66 Ingress protection rating

CD820F2

HD Compact fixed dome IP camera

- Multiple resolutions: 1080p/720p
- 1/2.7” Progressive scan CMOS imager
- Quad-stream H.264 and MJPEG video
- ONVIF compliant
- Audio - mic input
- 2.8 mm fixed lens
- Compact surface mount design
- Ruggedised construction
- 802.3af Power-over-Ethernet / 12 Vdc
- IP66 Ingress protection rating

IFD820V1IR

HD Indoor fixed dome IP camera

- 1/2.7” Progressive scan CMOS imager
- 3.0 - 10.5 mm Varifocal lens
- Multiple resolutions: 1080p/720p
- Quad-stream H.264 and MJPEG video
- Day/night with IR-cut filter
- Integrated IR illuminator (effective distance: 25 m)
- 24 Vac / 12 Vdc / 802.3af PoE
- ONVIF Profile S conformant

FD820M1 (-SFP)

HD Outdoor fixed dome IP camera

- 1/2.7” Progressive scan CMOS imager
- 3.0 - 10.5 mm Motorised varifocal lens
- Full HD 1080p resolution
- Quad-stream H.264 and MJPEG video
- Day/night with IR-cut filter
- IP66 Ingress protection rating
- 24 Vac / 12 Vdc / 802.3af PoE
- ONVIF Profile S conformant
- SFP interface (FD820M1-SFP)

FD820M1IR (-SFP)

HD Outdoor fixed dome IP camera

- 1/2.7” Progressive scan CMOS imager
- 3.0 - 10.5 mm Motorised varifocal lens
- Full HD 1080p resolution
- Quad-stream H.264 and MJPEG video
- Day/night with IR-cut filter
- Integrated IR illuminator (effective distance: 25 m)
- IP66 Ingress protection rating
- 24 Vac / 12 Vdc / 802.3af PoE
- ONVIF Profile S conformant
- SFP interface (FD820M1IR-SFP)

FD820M1IRMP5

HD Outdoor fixed dome camera

- 1/2.5" Progressive scan CMOS imager
- 3.3 to 10.5 mm Motorised lens with push-to-focus
- 5 Megapixel resolution
- Dual-stream H.264 and MJPEG video
- Day/night with IR-cut filter
- Integrated IR illuminator (effective distance: 25 m)
- IP66 Ingress protection rating
- 24 Vac / 12 Vdc / 802.3af PoE
- ONVIF Profile S conformant

3.2 Description

General

The Siqura CD/(I)FD820 is a network fixed dome camera providing high-quality high-definition images.

Multistream high definition

CD/(I)FD820 cameras support quad-stream (H.264 Baseline / Main / High Profile + MJPEG) or dual-stream (MP5 models) compression for efficient bandwidth and storage management. Multiple combinations of resolution and frame rate can be configured to satisfy different live viewing and recording scenarios. Full HD 1080p H.264 streaming with a D1 second stream or dual 720p streams is possible.

Open standards

Multiple options are available to easily integrate the CD/(I)FD820 into a video management system. In support of open standards, these cameras are compliant with the ONVIF Profile S specification in addition to Siqura's Open Streaming Architecture's (OSA) HTTP API.

Day/Night

(I)FD820 series cameras provide automatic day/night functionality, for use in low light situations. Under poor lighting conditions, the camera automatically becomes infrared-sensitive by removing the IR cut filter. This Day/Night feature ensures that even in minimal light the camera still produces clear images.

Backlight compensation

Backlight compensation enhances image visibility in difficult lighting conditions. In situations where the observed object is unclear due to being underlit or overlit (such as in a hallway entrance with many windows), backlight compensation improves image exposure by using the light near the object as a reference.

Wide dynamic range

Wide dynamic range solves the problem of overlit images by combining the best of two pictures with different light references.

Power source choices

The CD/(I)FD820 can be powered over the network with 802.3af compliant Power-over-Ethernet (PoE) sources (with the exception of the SFP model). IFD820 and FD820 units can also be powered by 12 Vdc or 24 Vac (terminal block).

Privacy masks

Privacy masks cover sections of the image. This feature is often requested for situations such as city centre surveillance and point of sale keypads.

4 Access the webpages

The webpages of the CD/(I)FD820 offer a user-friendly interface for configuring the settings of the unit and viewing live video images over the network. This chapter explains how to connect to the built-in web server.

In This Chapter

4.1 System requirements..... 14

4.2 Connect via web browser..... 14

4.3 Find the unit with Siqura Device Manager..... 15

4.4 Change the network settings with Siqura Device Manager..... 16

4.5 Log on to the unit..... 17

4.6 Install Siqura Viewer..... 18

4.7 The CD/(I)FD820 Web Interface..... 18

4.1 System requirements

You can log on to the webpages of the CD/(I)FD820 from a PC which is on the same subnet as the unit. Make sure that your PC has a good network connection and that it meets the following requirements.

Item	System requirement
Personal computer	• Intel® Pentium® M, 2.16 GHz or Intel® Core™2 Duo, 2.0 GHz • 2 GB RAM or more
Operating system	Windows 7
Web browser	Internet Explorere 6.0 or later, Firefox, Chrome, Safari
Network card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Internet Explorer

4.2 Connect via web browser

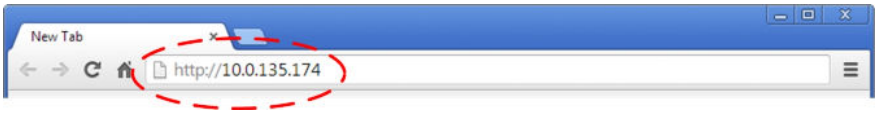
To connect to the unit via your web browser

1 Open your web browser.

2 Type the IP address of the CD/(I)FD820 in the address bar, and then press ENTER.

The factory-set IP address of the CD/(I)FD820 is in the 10.x.x.x range. You will find it printed on a sticker on the unit.

If your network configuration is correct you are directed to the login page of the unit.



Type the IP address of the CD/(I)FD820 in the address bar of the browser

Note: A hard reset sets the IP address of the camera to its factory-default setting (see above).

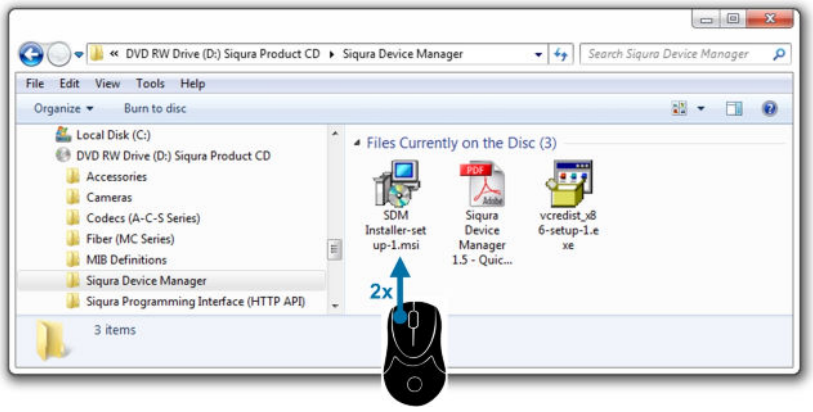
4.3 Find the unit with Siqura Device Manager

With Siqura Device Manager - a tool included on the supplied Siqura Product CD - you can locate, manage, and configure Siqura IP cameras and video encoders.

Note: Siqura Device Manager is also available for download at www.siqura.com.

To install Siqura Device Manager

1 Insert the supplied Siqura Product CD into your CD drive.
2 Browse to the Siqura Device Manager folder.
3 Double-click the setup file.
4 Follow the installation steps to install Siqura Device Manager.



Install Siqura Device Manager from the supplied CD

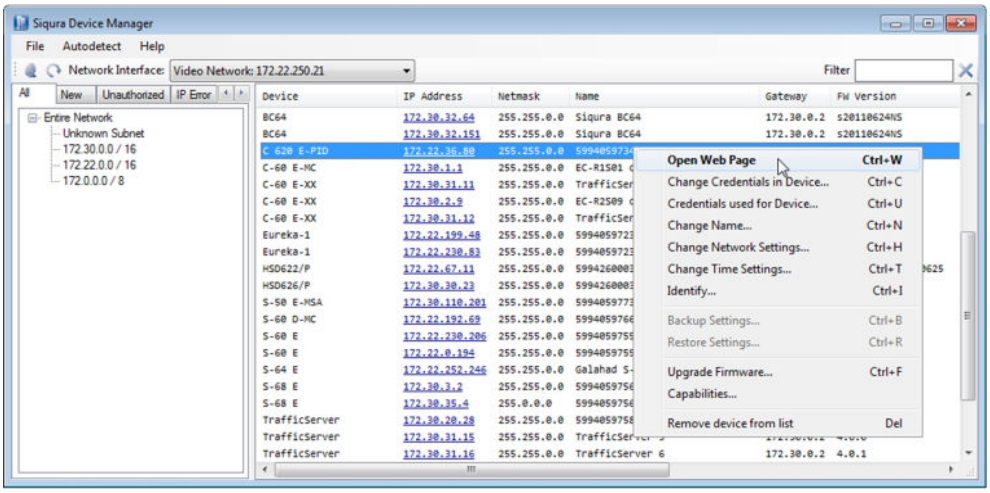
To connect to the unit via Siqura Device Manager

1 Start Siqura Device Manager
The network is scanned.
Detected devices appear in the List View pane.
2 If multiple network adapters exist, select the appropriate adapter to scan the network that you wish to connect to.
3 To perform a manual search, click the **Rescan** button.
4 Use the tabs in the *Tree View* pane to define the scope of your search.
5 Click the column headings in the *List View* pane to sort devices by type, IP address, or name.
6 To connect to the webpages of the CD/(I)FD820, double-click its entry in the device list,

- or -

Right-click the entry, and then click **Open Web Page**.

The login page of the CD/(I)FD820 is opened in your web browser.



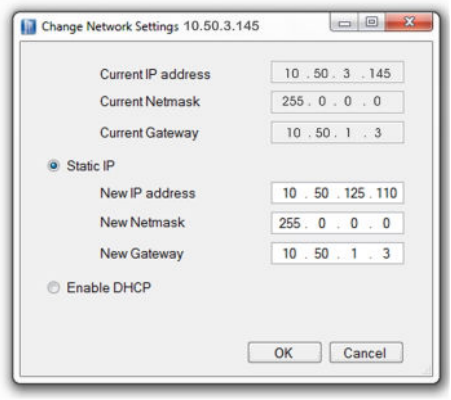
Connect to a device via Siqura Device Manager

4.4 Change the network settings with Siqura Device Manager

With Siqura Device Manager, you can directly change the network settings of the CD/(I)FD820.

To assign a static IP address

1. Go to the list of detected devices, and then right-click the entry for the CD/(I)FD820.
2. Click **Change Network Settings**.
3. In *Change Network Settings*, click **Static IP**.
4. Provide the camera with an appropriate IP address, netmask, and gateway address for the desired network configuration, and then click **OK**.
5. In the pop-up window indicating that you have successfully changed the settings, click **OK**.
6. Wait one minute, and then rescan the network.
7. To access the webpages of the CD/(I)FD820, double-click its entry in the list of found devices.



Assign a static IP address

To assign a DHCP server

1 Record the CD/(I)FD820's MAC address (see the *Serial no.* column in Siqura Device Manager) for future identification

2 In the list of detected devices, right-click the device with the network property that you would like to change.

3 Click **Change Network Settings**.

4 In *Change Network Settings*, click **Enable DHCP**, and then click **OK**.

5 In the pop-up window indicating that you have successfully changed the settings, click **OK**.

6 Wait one minute, and then rescan the network.

You can identify the device by its MAC address.

7 To access the webpages of the CD/(I)FD820, double-click its entry in the list of found devices.

Note: A DHCP server must be installed on the network in order to provide DHCP network support.

4.5 Log on to the unit

Users with a valid account for the CD/(I)FD820 can log on to the unit.

To log on

1 In the *Authentication* box, log on with the account that was created for you.

User name and password are case sensitive.

The default user name set at the factory for the CD/(I)FD820 is "Admin" with password "1234".

2 Click **Log In**.

Note: To prevent unauthorised access from people using the default account, we recommend that the administrator changes the default password after first login and creates separate user accounts as needed.

4.6 Install Siqura Viewer

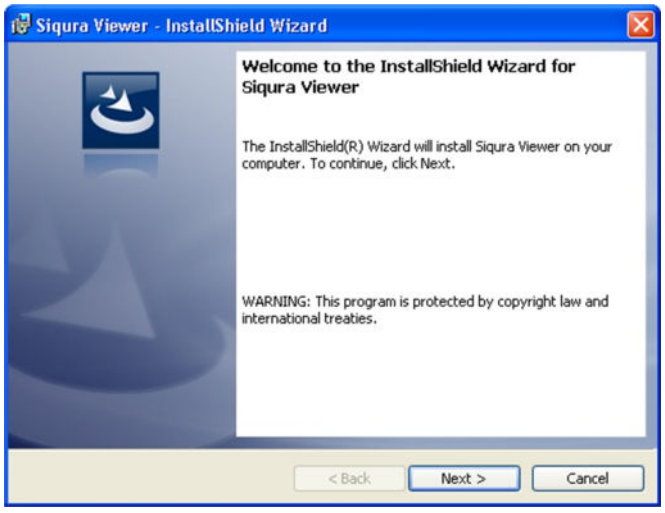
The first time you access the webpages of the camera, you may be prompted about the installation of Siqura Viewer. This add-on is required to view camera images in the webpages. The Siqura Viewer installation file is named `install.cab`. It does not give rise to any security risks. You can install it safely.

Important: You are strongly advised to remove a previous installation of Siqura Viewer from your computer before you initially access the camera over the network or when you encounter an "A new version is available" message. For more information, see *Appendix: Delete the existing Siqura Viewer software*.

Note: Make sure that the security settings of your web browser permit the use of ActiveX controls. For more information on how to modify these settings, see *Appendix: Set up Internet Security*.

To install the Siqura Viewer software

1. When prompted about the ActiveX control installation, allow the Siqura Viewer installation wizard to make changes to your computer.
2. In the initial screen of the installation wizard, click **Next**.
   A progress bar is displayed while the application is being installed.
3. When installation is complete, click **Finish**.
   The camera's web interface is displayed.


Siqura Viewer - InstallShield Wizard
Welcome to the InstallShield Wizard for Siqura Viewer
The InstallShield(R) Wizard will install Siqura Viewer on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

Siqura Viewer installation wizard

4.7 The CD/(I)FD820 Web Interface

On successful login, the home page of the CD/(I)FD820 is displayed. Camera settings and functions are organised on five main tabs found across the top of this page: **Home**, **System**, **Streaming**, **Camera**, and **Logout**.

Home

On the home page, users can monitor a live video stream from the camera and view stream details. This page is described in detail in the *Home* chapter.

System

From the System tab, administrators can view and configure system, security, and system related settings, and upgrade the embedded software. These settings are described in detail in the *System Settings* chapter.

Streaming

From the Streaming tab, administrators can set video and audio formats and compression parameters. These settings are described in detail in the *Streaming* chapter.

Camera

From the Camera tab, users can adjust various settings such as Exposure, White Balance, Picture Settings, Back Light Compensation, Digital Zoom, IR Function, Wide Dynamic Range, Noise Reduction, and TV System. These settings are described in detail in the *Camera* chapter.

Logout

The Logout option signs the user out of the camera's web pages and opens the Login page.

5 Home

This chapter describes the CD/(I)FD820 home page.

In This Chapter

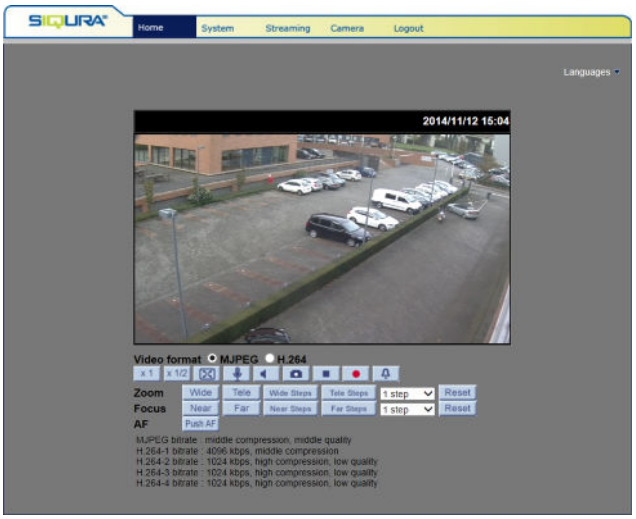
5.1 CD820/IFD820..... 20
5.2 FD820..... 21
5.3 Home page functions..... 22
5.4 Zoom and focus (FD820)..... 23

5.1 CD820/IFD820

CD820 and IFD820 home page

This Button	Does This
x 1	Sets image display to standard size
x 1/2	Sets image display to half size
	Sets image display to full screen
	Activates/mutes audio
	Saves a JPEG snapshot
	Pauses/Resumes video streaming
	Starts/Stops Live View recording
	Activates/Deactivates the manual trigger

5.2 FD820



FD820 home page

This Button	Does This
x 1	Sets image display to standard size
x 1/2	Sets image display to half size
	Sets image display to full screen
	Activates/deactivates the talk function
	Activates/mutes audio
	Saves a JPEG snapshot
	Pauses/Resumes video streaming
	Starts/Stops Live View recording
	Activates/Deactivates the manual trigger
Wide / Tele	Adjusts lens angle to wide angle / tele zoom position
Wide Steps / Tele Steps	Allows stepwise zoom adjustment
Near / Far	Adjusts lens focus to near/far position
Near Steps / Far Steps	Allows stepwise focus adjustment
1 step	Sets the range for stepwise zoom and focus adjustment
Reset	Sets the lens to full wide angle and infinity focus
Push AF	Activates one-push AF mode

5.3 Home page functions

On the home page, you can do the following:

- View live video
- Record live view images
- Save snapshots of live view images
- Adjust the video display size
- Select the video format
- Communicate with a remote site
- See details about the current video and audio
- Select a display language for the web pages

Languages

The CD/(I)FD820 web pages can be displayed in German, English, French, Italian, and Simplified Chinese. Select the desired language from the list in the upper-right corner of the page.

Screen size

Use the image display buttons to adjust the size of the camera view within the web page.

Digital zoom control

In full-screen mode, users can implement digital PTZ by rotating the mouse wheel to zoom in/out and dragging the mouse in any direction.

Audio

Using the Talk and Speaker buttons, you can communicate with a remote site. The associated audio functions are available to users with Talk and Listen privileges (assigned by the Administrator).

Snapshots

Pressing the Snapshot button saves a `.jpg` format snapshot of the video in the camera view to the configured location (default: `C:\`). For information about changing the storage location, see *File Location*.

Note: Users working with Windows 7 must log on as Administrator to implement the Snapshot function.

Pausing/Resuming video streaming

A blank screen displays when video streaming is paused. Press the Play button to resume video streaming.

Recording

Pressing the Recording button saves an `.avi` format recording of the video in the camera view to the configured location (default: `C:\`). For information about changing the storage location, see *File Location*.

Note: Users working with Windows 7 must log on as Administrator to implement the Recording function.

Manual trigger

The Manual trigger button activates the manual trigger function. For more information, see *Manual trigger*.

Info

In Normal View mode, double-clicking the camera view displays the Info box. This contains information about the current video and audio stream.

5.4 Zoom and focus (FD820)

FD820 series cameras support focus and zoom adjustment from the home page.

Zoom

Hold the Wide and Tele buttons for continuous zoom adjustment. Alternatively, you can click the Wide Steps and Tele Steps buttons for stepwise zoom adjustment using the step range selected on the drop-down list.

Focus

Hold the Near and Far buttons for continuous focus adjustment. Alternatively, you can click the Near Steps and Far Steps buttons for stepwise focus adjustment using the step range selected on the drop-down list.

Autofocus

A single mouse click on the Push AF button activates autofocus to fix the focus on the target in the camera view.

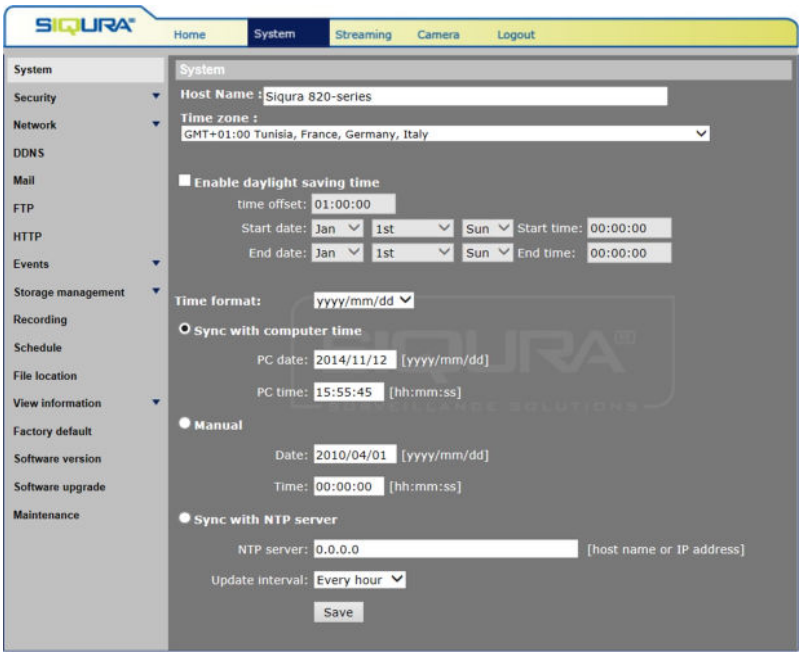
6 System settings

On the System tab, Administrators can set and modify the system parameters of the CD/(I)FD820. This chapter offers a detailed description of settings, options, and values found on this tab.

In This Chapter

6.1 System....25
6.2 Security....26
6.3 Network....33
6.4 DDNS....40
6.5 Mail....41
6.6 FTP....42
6.7 HTTP....43
6.8 Events....43
6.9 Storage management....56
6.10 Recording....60
6.11 Schedule....61
6.12 File location....62
6.13 View information....62
6.14 Factory default....66
6.15 Software version....67
6.16 Software upgrade....67
6.17 Maintenance....68

6.1 System



System > System

Clicking the System option in the left-hand panel displays the CD/(I)FD820's host name, time zone, time format, and time synchronisation settings. Remember to press **Save** after changing any settings.

6.1.1 Host name

Specify a name to identify the camera on the network. If the alarm function is enabled and set to send alarm messages by mail or FTP the host name entered here is displayed in the alarm message. The maximum length of the host name is 63 characters.

6.1.2 Time zone

On the Time zone list, select the time zone that corresponds with the location of the camera.

6.1.3 Daylight saving time

To enable daylight saving time

1. On the *System* tab, click **System** in the menu on the left.
2. Select **Enable daylight saving time**.
3. Specify the time offset.

   The format for the time offset is [hh:mm:ss]. If, for example, the time offset is 1 hour, enter `01:00:00` into the text box.
4. To set the daylight saving time duration, specify the **Start time** and **End time**.

6.1.4 Time format

Use the options on the Time format list to define how you wish to have date/time information displayed above the live video images in the webpages. Options: *yyyy/mm/dd* and *dd/mm/yyyy*.

6.1.5 Time synchronisation

To sync the displayed date and time with those of your PC

1 On the *System* tab, click **System** in the menu on the left.
2 Click **Sync with computer time**.
3 Click **Save**.
Note that the time will not be synchronised if you forget to click Save.

To set the displayed date and time manually

1 On the *System* tab, click **System** in the menu on the left.
2 Click **Manual**.
3 Enter the date and time
Note that the entry format for date and time should match the one shown next to the entry field (yyyy/mm/dd).
This in its turn is determined by the format that is selected on the Time format list.
4 Click **Save**.

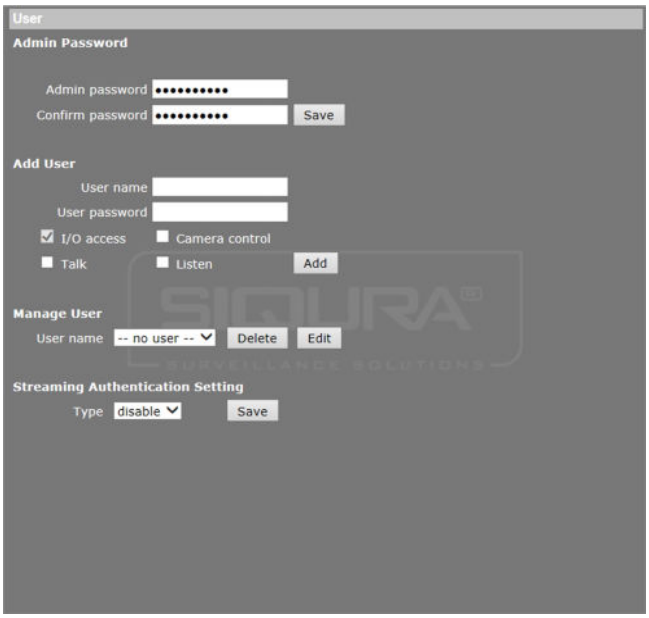
To sync with an NTP server

1 On the *System* tab, click **System** in the menu on the left.
2 Select **Sync with NTP server**.
The Network Time Protocol (NTP) will be used to synchronise the clock of the camera with an NTP server. For more information, refer to the website of NTP (see - http://www.ntp.org).
3 Enter the IP address or host name of the NTP server.
4 Select an update interval.
5 Click **Save**.
Every time the camera boots up, it will be synchronised.

6.2 Security

From the Security pages, the administrator can perform user management, install security certificates, and enable and configure an IP address filter.

6.2.1 User



System > Security > User

6.2.1.1 Admin password

The default user name is Admin. The default password is 1234. User name and password are case sensitive. It is recommended that the administrator change the default password.

To change the administrator password

1 On the *System* tab, click **Security** in the menu on the left.

2 In the *Security* submenu, click **User**.

3 Type the new password in the *Admin password* and *Confirm password* text boxes.

Maximum password length is 14 characters. For security purposes, this input is displayed as dots.

Note: The following characters are valid: A-Z, a-z, 0-9, ! # $ % & ' - . @ ^ _ ~

4 Click **Save**.

The web interface prompts the administrator for the new password for continued access.

6.2.1.2 Add and manage user accounts

The camera supports a maximum of twenty user accounts. User names can be up to 16 characters. Passwords can be up to 14 characters. Each user can be assigned the privileges of *Camera control*, *Talk* (if supported by the camera), and *Listen*.

Privilege	Description
I/O access	This privilege, granted by default, supports fundamental functions that enable users to view live video when accessing the camera.
Camera control	This privilege allows the user to change parameters on the Camera tab and Pan Tilt tab.
Talk/Listen	The Talk and Listen functions allow the user to communicate from the local machine with, for example, the administrator on a remote site.

To add a user

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **User**.
3 In the *Add User* section, type the new user's name and password.
4 Select the **Camera control**, **Talk** (if supported), and **Listen** check boxes, as appropriate, to set the user's permissions.
Permission to view the home page and operate its controls is granted, by default, to all users.
5 Click **Add** to add the new user.
The new user is displayed in the User name list.

To delete a user

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **User**.
3 In the *Manage User* section, select the name of the user that you want to delete.
4 Click **Delete** to remove the user.
The application takes about 20 seconds to delete the user.

To edit a user's password and privileges

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **User**.
3 In the *Manage User* section, select the name of the user and click **Edit**.
4 In the dialog box, select/clear the user's permissions and/or change the user's password.
Note that every user account requires a password and defined permissions.
5 Click **Save** to confirm settings.

6.2.1.3 Streaming Authentication Setting

This function is disabled by default. Users can freely open an RTSP connection to the CD/(I)FD820 and extract a video stream. This may be undesirable from a security perspective. Therefore, it is possible to restrict access to the CD/(I)FD820 to users with a valid account.

To enable Streaming Authentication

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **User**.
3 Under *Streaming Authentication Setting*, click the **Type** list.

4 Click **basic** or **digest**, as required (see below).

5 Click **Save**.

On attempting to open a video stream, users will now be asked to provide a user name and password.

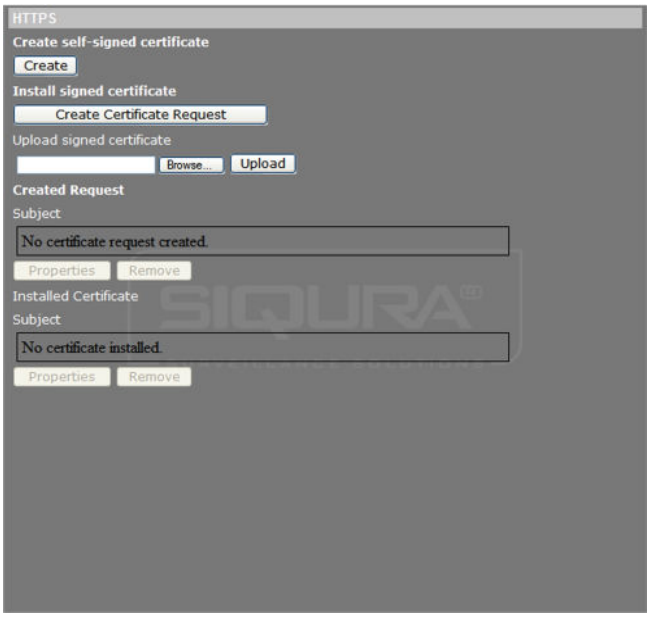
Basic mode

Basic access authentication transmits user names and passwords as plain text. Therefore, it should only be used where security is provided by HTTPS.

Digest mode

Digest authentication communicates credentials in an encrypted form and is therefore a safer option for protection.

6.2.2 HTTPS



System > Security > HTTPS

HTTPS, SSL, and TLS

Hypertext Transfer Protocol Secure (HTTPS) allows secure connections between the IP camera and the web browser using Secure Socket Layer (SSL) or Transport Layer Security (TLS), which protect camera settings and user name / password information from eavesdropping.

To implement and use HTTPS on the camera, an HTTPS certificate must be installed. This can be obtained by creating and sending a certificate request to a Certificate Authority (CA). Before a CA-issued certificate is obtained, users can create and install a self-signed certificate first.

Note: The self-signed certificate does not provide the same high level of security as when using a CA-issued certificate.

6.2.2.1 Create a self-signed certificate

To create a self-signed certificate

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **HTTPS**.
3 Under *Create self-signed certificate*, click **Create**.
4 Enter the requested information in the *Create* dialog box, as described below.
All fields are required.
5 After completing the form, click **OK** to save the certificate information.

Field	Description
Country	Enter a 2-letter combination code to indicate the country the certificate will be used in. For example, type "US" to indicate the United States.
State or province	Enter the local administrative region.
Locality	Enter other geographical information.
Organisation	Enter the name of the organisation to which the entity identified in "Common Name" belongs.
Organisational unit	Enter the name of the organisational unit to which the entity identified in "Common Name" belongs
Common name	Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
Valid days	Enter the period in days (1~9999) to indicate the valid period of certificate.

6.2.2.2 Create and install a signed certificate

To create a signed certificate request

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **HTTPS**.
3 To create request to obtain a signed certificate from a CA, click **Create Certificate Request**.
4 Enter the requested information in the *Create Certificate Request* dialog box, as described above.
For a signed certificate from a CA, the *Valid days* field does not apply.
5 After completing the form, click **OK** to save the certificate information.
The subject of the created request is shown in the Subject field.
6 Click **Properties**.
7 Copy the PEM-formatted request and send it to your selected CA.

To install a signed certificate received from a CA

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **HTTPS**.
3 Under *Upload signed certificate*, click **Browse**.
4 Browse to the folder containing the signed certificate and select the file.
5 Click **Upload**.

The certificate is installed and displayed under Installed Certificate.

6.2.3 IP filter

System > Security > IP filter

Using the IP filter, you can deny/allow access to the IP camera from specific IP addresses. Up to 256 IP addresses may be specified.

To enable the IP filter

1 On the *System* tab, click **Security** in the menu on the left.
2 In the *Security* submenu, click **IP filter**.
3 Select **Enable IP filter**.
4 To determine the IP filter behaviour, select **Deny** or **Allow** from the list.
5 Click **Apply**.
IP addresses listed under Filtered IP Addresses are now allowed/denied access to the camera.

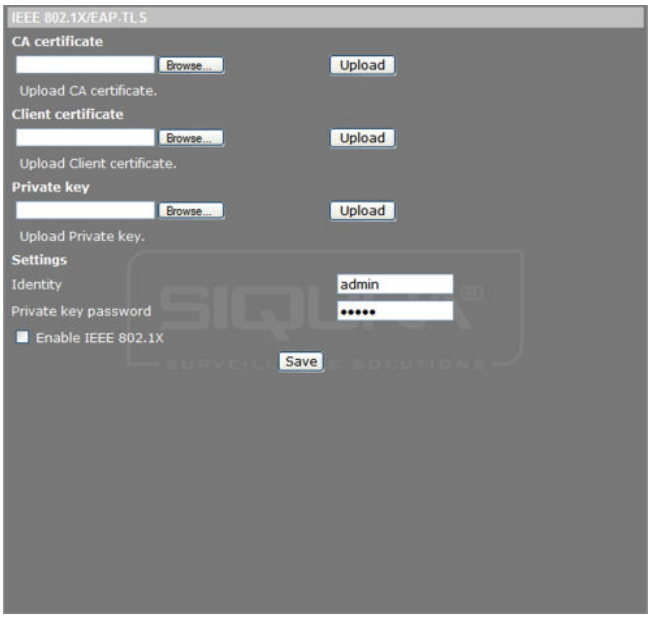
To add an IP address

1 Enter the IP address.
2 Click **Add**.
The address is added to the currently configured IP addresses.
Up to 256 IP addresses can be specified.

To delete an IP address

1 Select the IP address.
2 Click **Delete**.
The IP address is removed from the list.

6.2.4 IEEE 802.1X



System > Security > IEEE 802.1X

The CD/(I)FD820 is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). Users need to contact the network administrator to obtain certificates, User IDs, and passwords.

6.2.4.1 CA certificate

The CA certificate is created by the Certificate Authority (CA) for validation purposes. Upload the certificate to verify the server's identity.

To install a CA certificate

1. On the *System* tab, click **Security** in the menu on the left.
2. In the *Security* submenu, click **IEEE 802.1X**.
3. Under *CA certificate*, click **Browse**.
4. Browse to the folder containing the certificate and select the file.
5. Click **Upload**.
   The certificate is installed.

6.2.4.2 Client certificate and private key

The Client certificate and Private key must be uploaded to authenticate the camera itself.

To upload a Client certificate / Private key

1. On the *System* tab, click **Security** in the menu on the left.
2. In the *Security* submenu, click **IEEE 802.1X**.
3. Under Client certificate/Private key, click **Browse**.
4. Browse to the folder containing the certificate/key and select the file.
5. Click **Upload**.
   The certificate/key is installed.
6. In the *Identity* text box, enter the user identity associated with the certificate.

Up to 16 characters can be used.

7 In the *Private key password* text box, enter the password for your user identity.
Up to 16 characters can be used.

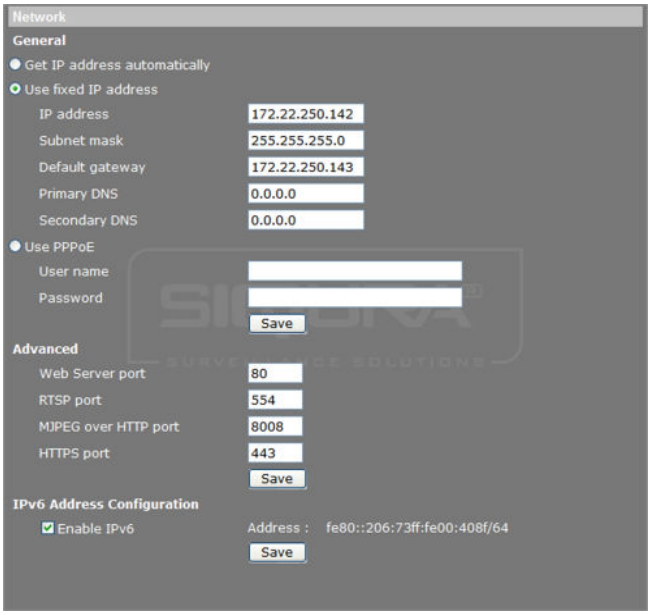
8 To enable IEEE 802.1X, select **Enable IEEE 802.1x**.

9 Click **Save**.

6.3 Network

From the Network pages, the administrator can configure IP address assignment and settings for Quality of Service (QoS), the Simple Network Management Protocol (SNMP), and Universal Plug and Play (UPnP).

6.3.1 Basic



System > Network > Basic

This page describes how to configure the camera to use a fixed IP address or acquire the address dynamically through the Dynamic Host Configuration Protocol (DHCP). You can also configure PPPoE support, Advanced network settings, and enable IPv6 support.

Note: When the IP address is changed, webpage communication is lost. Log on to the webpage with the new address to re-establish the connection.

6.3.1.1 Acquire an IP address automatically

By default, the CD/(I)FD820 cameras are configured to use a fixed IP address. Administrators can set the camera to obtain its IP address via the Dynamic Host Configuration Protocol (DHCP).

Note: When an IP address changes, cameras using DHCP can always be identified by their MAC address, found on the camera's label. You are advised to keep the MAC address on record for future identification.

To acquire the IP address via DHCP

1 On the System tab, click **Network** in the menu on the left.
2 In the *Network* submenu, select **Basic**.
3 Click **Get IP address automatically**.
4 Click **Save** to confirm the new setting.
The camera restarts automatically.
Use Siqura Device Manager (supplied on the Siqura Product CD) to find the camera on the network.

6.3.1.2 Modify the fixed IP address

The factory default IP address is in the 10.x.x.x range.

To modify the camera's fixed IP address

1 On the System tab, click **Network** in the menu on the left.
2 In the *Network* submenu, select **Basic**.
3 Select **Use fixed IP address**.
4 In the *IP address* box, type the camera's IP address.
5 Enter the subnet mask, default gateway, and DNS server IP addresses in the appropriate boxes.
See below for more detailed information.
6 Click **Save** to confirm the new settings.
7 Enter the new IP address in the address bar of your web browser, and then press **Enter** to re-establish communication with the camera.
- or -
Find the camera with `Siqura Device Manager`.

IP address

The IP address identifies the camera on the network.

Subnet mask

The subnet mask is used to determine if the destination is on the same subnet. The default value is 255.0.0.0.

Default gateway

The default gateway is used to forward frames to destinations on other subnets. If the gateway setting is invalid, transmissions to destinations on other subnets will fail.

DNS

The primary DNS is the primary domain name server that translates host names into IP addresses. The secondary DNS is a second domain name server that is used if the primary DNS is unavailable.

6.3.1.3 Use PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) enables users to securely transfer data.

To use PPPoE

1 On the System tab, click **Network** in the menu on the left.
2 In the *Network* submenu, select **Basic**.
3 Click **Use PPPoE**.
4 Specify the PPPoE user name and password.
5 Click **Save**.

6.3.1.4 Advanced settings

Web Server port

The HTTP port can be any port other than the default port, 80. If the port is changed, the user must be notified of the change for connections to be successful.

For example, if the administrator changes the HTTP port of a camera with an IP address of 192.168.0.100 from 80 to 8080, the user must type in the address http://192.168.0.100:8080 instead of http://192.168.0.100.

RTSP port

The RTSP port can be any port other than the default port, 554. If the port is changed, the user must be notified of the change for connections to be successful. The port number may range from 1024 to 65535.

For example, if the administrator changes the RTSP port of a camera with an IP address of 192.168.0.100 from 554 to 8080, the user must type in the address rtsp://192.168.0.100:8080 instead of rtsp://192.168.0.100.

MJPEG over HTTP port

The HTTP port that streams MJPEG can be any port other than the default port, 8008. If the port is changed, the user must be notified of the change for connections to be successful. The port number may range from 1024 to 65535.

For example, if the administrator changes the MJPEG over HTTP port of a camera with an IP address of 192.168.0.100 from 8008 to 8080, the user must type in the address http://192.168.0.100:8080 instead of http://192.168.0.100.

HTTPS port

The HTTPS port can be any port other than the default port, 443. If the port is changed, the user must be notified of the change for connections to be successful. The port number may range from 1024 to 65535.

For example, if the administrator changes the HTTPS port of a camera with an IP address of 192.168.0.100 from 443 to 650, the user must type in the address https://192.168.0.100:650 instead of https://192.168.0.100.

Note: Be aware that a different port must be chosen from the one set for the Web Server port.

6.3.1.5 IPv6 address configuration

To enable IPv6 support

1 On the System tab, click **Network** in the menu on the left.

2 In the *Network* submenu, select **Basic**.

3 Under *IPv6 Address Configuration*, select **Enable IPv6**.

4 Click **Save**.

The IPv6 IP address is displayed.

6.3.2 QoS

System > Network > QoS

DiffServ and QoS

Differentiated Services (DiffServ, or DS) is a method for adding Quality of Service (QoS) to IP networks. In routed networks, critical network traffic such as video and audio streams, which require a relatively uninterrupted flow of data, can get blocked due to other traffic. DiffServ can be used to classify network traffic and give precedence - that is, low-latency, guaranteed service, to high-priority traffic, while offering best-effort service to non-critical traffic such as file transfers or Web traffic.
Each stream has a DSCP (Differentiated Services Code Point) field in the IP header. Routers will identify the network service type in the DSCP field and provide the appropriate level of service. Low-latency service can be realised, for example, through priority queuing, bandwidth allocation, or by assigning dedicated routes.

DSCP settings

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled. The IP camera uses the following QoS Classes: Video, Audio, and Management.

Video DSCP

The class consists of applications such as MJPEG over HTTP, RTP/RTSP, and RTSP/HTTP.

Audio DSCP

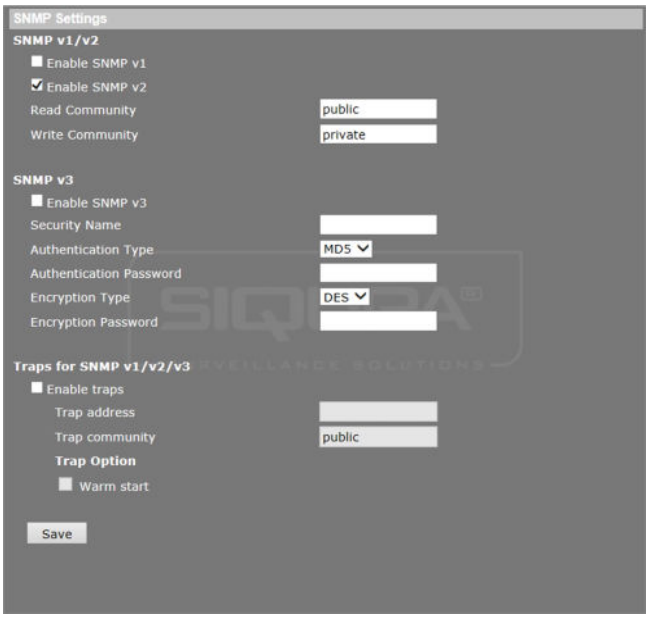
This setting is available for IP cameras that support audio.

Management DSCP

The class consists of HTTP traffic: Web browsing.

Note: Before enabling this function, make sure the switches/routers in the network support QoS.

6.3.3 SNMP



System > Network > SNMP

With the Simple Network Management Protocol (SNMP), part of the internet protocol suite, the CD/(I)FD820 can be monitored and managed remotely by a network management system.

SNMP v1/v2

To enable the version of SNMP to use, select the appropriate check box.

Read Community

Specify the community name that has read-only access to all supported SNMP objects. The default value is "public".

Write Community

Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is "private".

SNMP v3

SNMP v3 supports an enhanced security system that provides protection against unauthorised users and ensures the privacy of the messages. Users will be requested to enter a security name, authentication password and encryption password while setting the camera connections in the network management system. With SNMP v3, the messages sent between the cameras and the network management system will be encrypted to ensure privacy.

Enable SNMP v3

To enable this version of SNMP, select the check box.

Security Name

The maximum length of the security name is 32 characters.

Note: The valid characters are A-Z, a-z, 0-9, !#$%&'-.@^_~.

Authentication Type

There are two authentication types available: MD5 and SHA. Select SHA for a higher security level.

Authentication Password

The authentication password must be eight characters or more. The input characters / numbers will be displayed as dots for security purposes.

Note: The valid characters are A-Z, a-z, 0-9, !#$%&'-.@^_~.

Encryption Type

There are two encryption types available: DES and AES. Select AES for a higher security level.

Encryption Password

The minimum length of the encryption password is eight characters and the maximum length is 512 characters. The input characters / numbers will be displayed as dots for security purposes. The encryption password can also be left blank. In that case, the messages will not be encrypted to protect privacy.

Note: The valid characters are A-Z, a-z, 0-9, !#$%&'-.@^_~.

Traps for SNMP v1/v2/v3

Traps are used by the CD/(I)FD820 to send messages to a management system to report important events or status changes.

Enable traps

Selecting the check box activates trap reporting.

Trap address

Enter the IP address of the management server.

Trap community

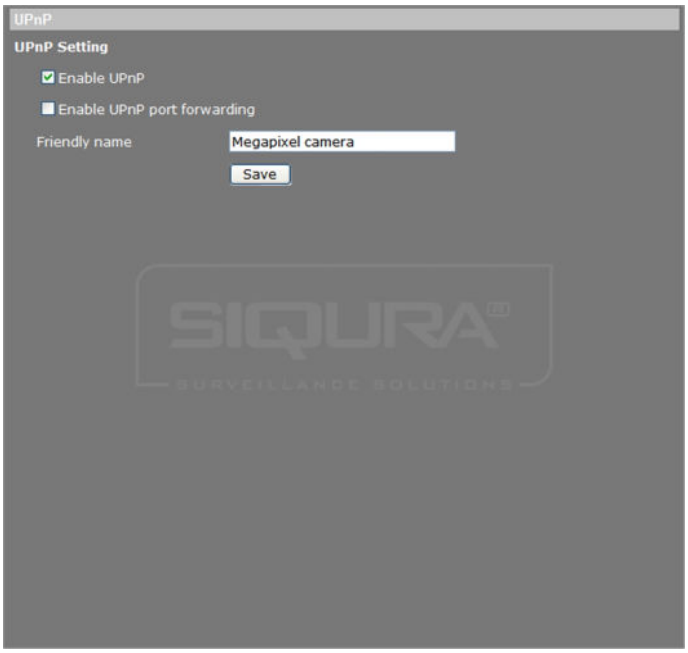
Enter the community to use when sending a trap message to the management system.

Trap option

A Warm Start SNMP trap signifies that the SNMP device - that is, the CD/(I)FD820, reinitialises itself by performing a software reload, such that its configuration is unaltered.

Note: Remember to click the **Save** button, after modifying settings on this page.

6.3.4 UPnP



System > Network > UPnP

Enable UPnP

If enabled, Universal Plug and Play (UPnP) allows the CD/(I)FD820 to advertise its presence and services to control points on the network. A control point can be a network device with embedded UPnP or a Video Management System (VMS). The icon of the CD/(I)FD820 will appear in *My Network Places* to allow direct access.

Note: To access the camera from your computer through UPnP, ensure that the UPnP networking service is installed on your computer. Please refer to *Appendix A: Enable UPnP Components in Windows 7* for the UPnP installation procedure.

Enable UPnP port forwarding

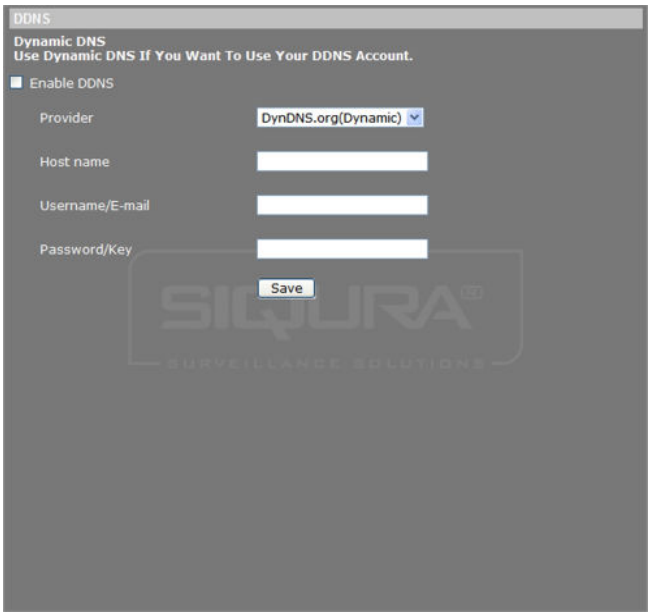
When UPnP port forwarding is enabled, the CD/(I)FD820 is allowed to open the web server port on the router automatically.

Note: To enable this function, ensure that your router supports UPnP and that the function is activated.

Friendly name

Set the name that the CD/(I)FD820 will use to identify itself on the network.

6.4 DDNS



System > DDNS

The Dynamic Domain Name System (DDNS) allows a DNS name to be constantly synchronised with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated with a static domain name.

To use DDNS

1 From the Network page, set the camera to acquire its IP address via DHCP, as described in *Acquire an IP address automatically*.

2 On the *System* tab, click **DDNS** in the menu on the left.

3 Click to select the **Enable DDNS** check box.

4 Select the DDNS provider from the *Provider* list.

5 Type the registered domain name in the *Host name* box.

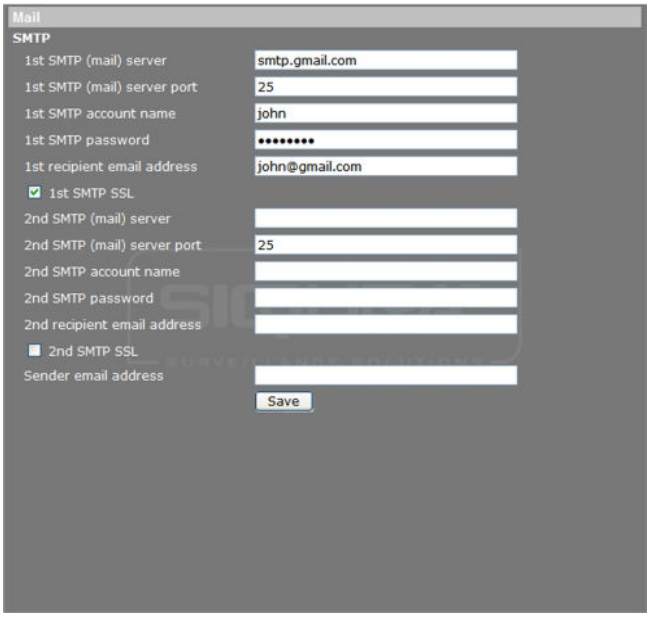
> **Note:** Only enter the desired third-level host name into the box. For example, if the host name is hsd820.dyndns.org, then enter hsd820.

6 In the *User name/E-mail* box, type the user name or e-mail required by the DDNS provider for authentication.

7 In the *Password/Key* box, type the password or key required by the DDNS provider for authentication.

8 Click **Save** to confirm settings.

6.5 Mail



System > Mail (example settings)

On the Mail page, administrators can configure SMTP settings for sending an email via the Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. SMTP is a protocol for exchanging email messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

To configure SMTP settings

1 On the *System* tab, click **Mail** in the menu on the left.

2 Enter the following SMTP details:

- 1st SMTP (mail) server (IP address or host name)
- 1st SMTP (mail) server port (21 is the default port for FTP servers)
- 1st SMTP account name
- 1st SMTP password
- 1st recipient email address (entire email address limited to 64 characters)
- If the server requires a secure connection (SSL), select **1st SMTP SSL**

3 If desired, repeat step 2 for the second SMTP configuration.

4 Click **Save**.

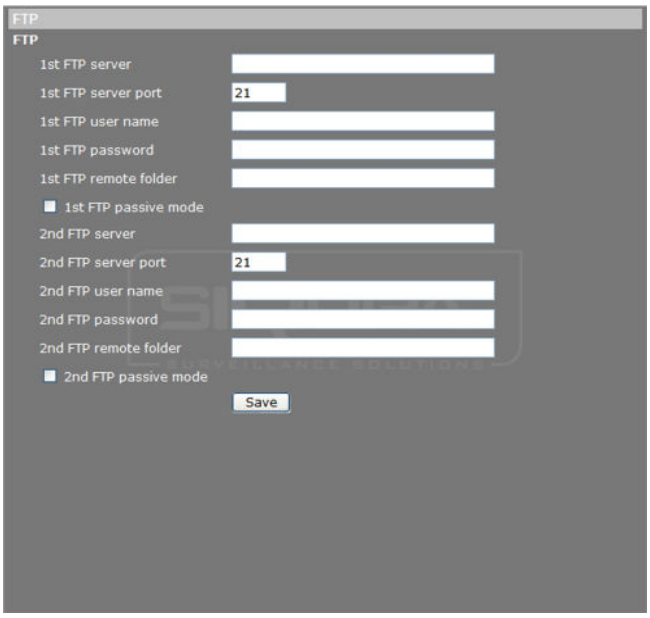
SMTP server

For SMTP server details (IP address or name), contact your network service provider or network administrator.

Sender email address

The sender's email address will be displayed in the alarm triggered email or FTP message.

6.6 FTP



System > FTP

Administrators can configure the camera to send messages to one or two specific File Transfer Protocol (FTP) sites when an alarm is triggered. For FTP server details, contact your network administrator or network service provider, or install FTP software on a PC on the same network as the camera.

To configure FTP settings

1 On the *System* tab, click **FTP** in the menu on the left.

2 Enter the following FTP details:

- Server (IP address or host name)
- Server port (21 is the default port for FTP servers)
- User name (from the account created on the FTP server)
- Password
- Remote folder

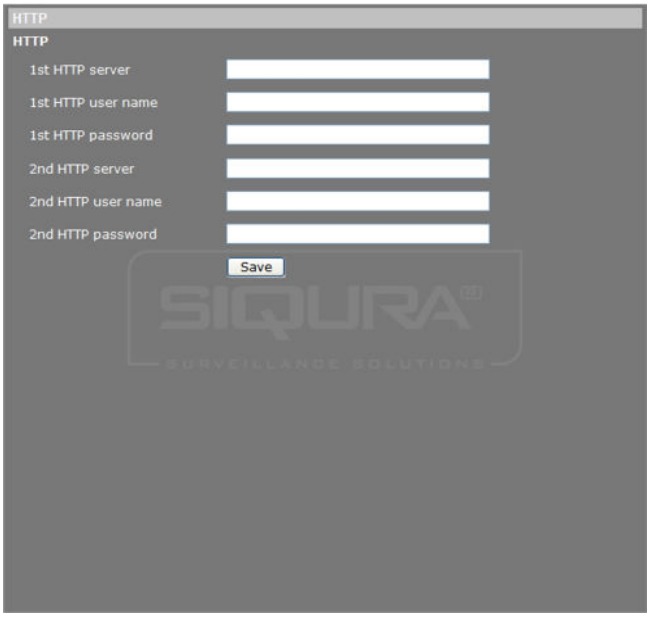
Note: Do not enter the complete FTP path into the remote folder field. For example, if the remote folder is `C:\FTP\example\` and the FTP path is `C:\FTP\`, then only the word 'example' should be entered.

3 Enable the 1st FTP passive mode or the 2nd FTP passive mode or both, if necessary.

In passive mode, the relevant FTP server initiates a connection with the FTP client by sending its IP address through a dynamic port. In active mode, the FTP client initiates the connection.

4 Press **Save** when finished.

6.7 HTTP



System > HTTP

An HTTP Notification server can listen for notification messages from IP cameras triggered by events. Alarm triggered and motion detection notifications can be sent to the specified HTTP server. See also Application, Motion Detection, and Tampering for HTTP Notification settings.

To configure HTTP settings

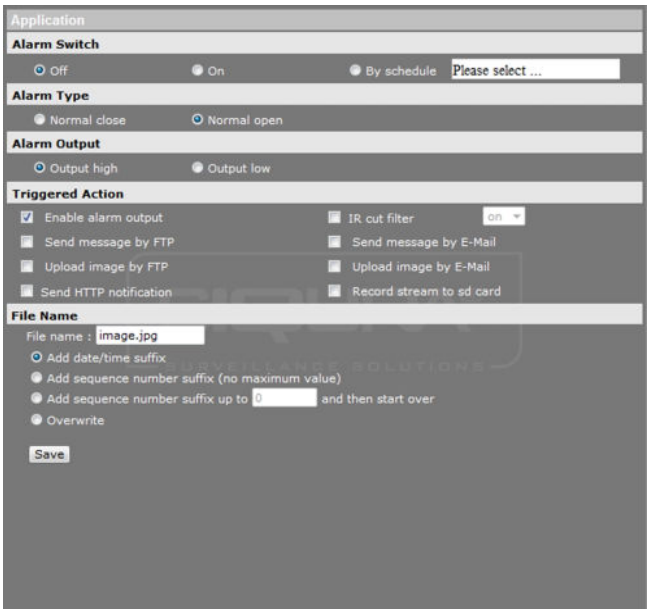
1 On the *System* tab, click **HTTP** in the menu on the left.
2 Enter the following HTTP details:
- HTTP server (for example, http://192.168.0.1/admin.php)
- User name
- Password

3 Click **Save** when finished.

6.8 Events

The Events menu gives access to the Application (FD820), Motion detection, Network failure detection, Tampering, Periodical event, Manual trigger, and Audio detection webpages.

6.8.1 Application



System > Events > Application (FD820)

The FD820 provides one digital alarm input and one digital alarm output to be used with an alarm and its specified trigger actions.

On the Application page, administrators can set the active state of the digital input and output (I/O), enabling the camera to trigger an alarm when the state of the alarm connector changes.

To set up alarm settings

1 On the *System* tab, click **Events** in the menu on the left, and then click **Application**.

2 Under *Alarm Switch*, select **On,** or **Off** to enable or disable the alarm input and the actions triggered by it.

Alternatively, you can select *By schedule* and then select a schedule that you have configured through the *Schedule* page.

3 On the *Alarm type* list, select the alarm input type, either **Normal close** or **Normal open**, according to the application. See below for more details.

4 Under *Triggered Action*, select the actions that are to be performed in the event of an alarm. For more information, see T*riggered Action*.

5 If applicable, under *File name*, specify a file name for a file to be sent when an alarm occurs, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.

6 Click **Save**.

SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions.

Important: Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

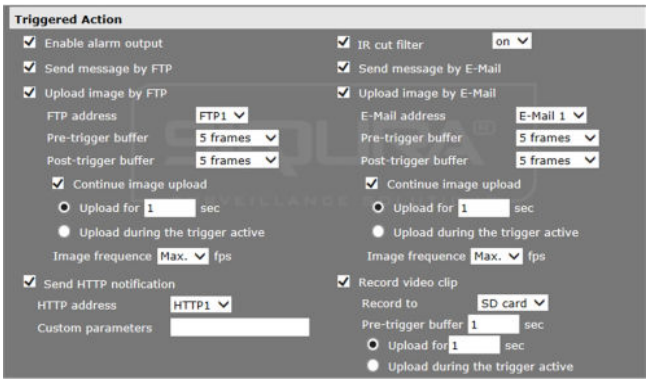
Alarm Type

The input type drives the alarm output. *Normal close* indicates that the connectors are normally closed and a disconnection will trigger a digital output signal. *Normal open* indicates that the connectors are normally open and a connection will trigger a digital output signal. See the relevant installation manual for more information.

Alarm Output

The alarm output can be enabled under *Triggered Action*. Select *Output high* or *Output low* as the normal alarm status according to the current alarm application.

6.8.1.1 Triggered action



System > Application > Triggered Action

The actions detailed in this section can be set to be triggered when an alarm occurs. Ensure that the SMTP, FTP, and/or HTTP configuration is complete prior to configuring an alarm's triggered actions.

Enable alarm output (FD820)

The FD820 provides one alarm output. It can be enabled by selecting the *Enable alarm output* check box.

Send message by FTP

A message is sent to the FTP site, as configured on the FTP page, when an alarm is triggered. For more information on how to configure messages to be sent to an FTP site, see *FTP*.

Upload image by FTP

When an alarm is triggered, a specified number of pre- and post-trigger buffer frames are sent to the configured FTP server. This allows users to check what happened to cause the trigger.

Important: Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

Continue image upload (by FTP)

If selected you can choose from the following actions:

- Upload for n sec

  The number of frames per second (fps) selected from the *Image Frequence* list is sent to the FTP Server for the number of seconds specified in the *Upload for n sec* box.
- Upload during trigger active

  The number of frames per second (fps) selected from the *Image Frequence* list is sent to the FTP Server until the trigger is no longer active.

Send HTTP notification

An HTTP Notification Server can listen for notification messages from IP cameras. The CD/(I)FD820 can send event-triggered notifications to the server selected from the *HTTP address* list.

To enable the sending of HTTP notifications

1 Select **Send HTTP notification**.

2 Click to open the **HTTP address** list, and then select an HTTP server.

3 In the *Custom parameters* text box, specify the parameters for event notifications.

If, for example, the custom parameter is set as "action=1&group=2" and the HTTP server name is "http://192.168.0.1/admin.php", the notification will be sent to the HTTP server as "http://192.168.0.1/admin.php?action=1&group=2" when an alarm is triggered.

IR cut filter (on supported units)

Select this check box to have the camera's IR cut filter removed (on) or returned (off) when the alarm input is triggered.

Note: The IR function cannot be set to Auto if this triggered action is enabled.

Send message by E-mail

A message is sent by e-mail, as configured on the Mail page, when an alarm is triggered. For more information on configuring messages to be sent via SMTP, see *Mail*.

Upload Image by E-mail

When an alarm is triggered, a specified number of pre- and post-trigger buffer frames are sent in an e-mail. This allows users to check what happened to cause the trigger.

Continue image upload (by E-mail)

If selected you can choose from the following actions:

- Upload for n sec

  E-mails are sent for the number of seconds specified in the *Upload for n sec* box. Each e-mail contains the number of frames per second (fps) selected from the *Image Frequence* list.

- Upload during trigger active

  E-mails are sent until the trigger is no longer active. Each e-mail contains the number of frames per second (fps) selected from the *Image Frequence* list.

Record video clip

Using the options on the *Record t*o list, you can have an alarm-triggered recording saved to your microSD card or NAS. The Pre-trigger buffer function allows you to check what occurrence caused the trigger. The Pre-trigger buffer time range is from 1 to 3 seconds.

You can choose from the following actions:

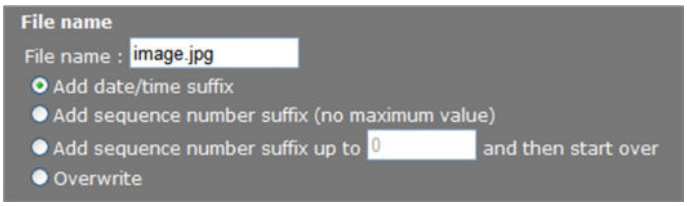
- Upload for n sec

  The image stream is recorded to the SD card for the number of seconds (setting range from 1 to 99999 seconds) specified in the *Upload for n sec* text box with a pre-trigger buffer of the number of seconds specified in the *Pre-trigger buffer* text box.

- Upload during trigger active

  The image stream is recorded to the SD card with a pre-trigger buffer of the number of seconds specified in the *Pre-trigger buffer* text box until the trigger is no longer active.

6.8.1.2 Specifying file name conventions


File name
File name : image.jpg
Add date/time suffix
Add sequence number suffix (no maximum value)
Add sequence number suffix up to 0 and then start over
Overwrite

Application > Alarm pin# status > File name

The File Name text box allows users to specify the file name conventions for captured images. The following options are available for naming image files.

- *File name*

  Enter a file name for the uploaded images. For example, image.jpg. A suffix will be added unless Overwrite is selected.

- *Add date/time suffix*

  An incremented sequence number and the date and time of when an image is captured are added to the end of the file name. The date, time, and sequence number are provided as follows.

- imageYYMMDD_HHNNSS_XX.jpg, where Y: Year, M: Month, D: Day, H: Hour, N: Minute, S: Second, X: Sequence Number

- *Add sequence number suffix (no maximum value)*

  An incremented sequence number is added to the end of the file name. The sequence number is unlimited.

- *Add a sequence number suffix up to n and then start over*

  An incremented sequence number is added to the end of the file name. The numbering is reset when it reaches the given maximum value, at which point images from previous numbering cycles will be overwritten.

- *Overwrite*

  The latest uploaded image file with a static file name will overwrite the previous image.

6.8.2 Motion detection

System > Events > Motion detection

The Motion Detection function enables the camera to trigger an alarm when motion in a specified area reaches or exceeds a configured sensitivity threshold value.

Note: To prevent false alarms, Motion Detection is disabled during PTZ control and when working with presets and sequences, and cruises.

To enable the Motion Detection alarm

1 On the *System* tab, click **Events** in the menu on the left, and then click **Motion detection**.

You can configure up to four sets of Motion Detection settings.

2 On the *Motion Detection* list, select the Motion Detection instance that you want to configure, and then click **On**.

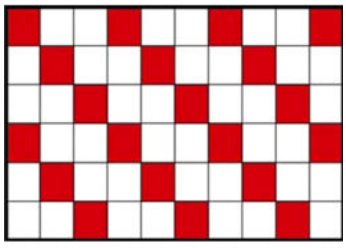
The default setting is *Off*.

Alternatively, you can set up Motion Detection activity by clicking *By schedule* and selecting a schedule that you have configured through the *Schedule* page.

3 Under *Motion Detection Setting*, enter values for the following parameters.

- Sampling pixel interval [1-10]

  The default value is 1. If the value is set to 3, for example, the system will take one sampling pixel for every 3 pixels per each row and each column within the detection region.



- Detection level [1-100]

The default level is 10. This parameter sets the detection level for the sampling pixels. The lower the value, the more sensitive the detection level is.

- Sensitivity level [1-100]

  The default level is 80, which means that if 20% or more pixels in the detection window change, the system will detect motion. The higher the value, the more sensitive it is. As the value increases, the red horizontal line in the motion indication window will lower accordingly.

- Time interval (sec) [0-7200]

  The default interval is 10. This value is the duration in seconds between each detected motion.

4 Under *Triggered action*, select the desired trigger actions that are to be performed in the event of an alarm. For more information, see *Triggered Action*.

5 If applicable, under *File name*, specify a file name for a file to be sent when an alarm occurs, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.

6 Click **Save**.

SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions. For more information, see *Mail*, *FTP*, and/or *HTTP*.

Important: Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

6.8.2.1 Motion detection area

On the Motion Detection page, up to ten motion detection areas can be added. A red frame displays in the camera view around the selected detection area. These areas can be added removed, moved, and/or resized.

Motion detection with two windows configured

To add a motion detection area

- Click **add**.

To remove a motion detection area

- Select the area, and then click **delete**.

To resize a motion detection area

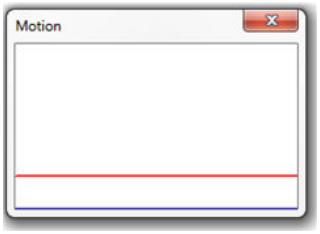
- Point to the edge of the red frame and drag the pointer to modify the motion detection area's size.

To move the motion detection frame

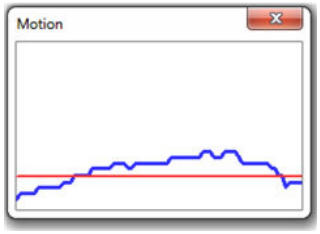
- Press and hold the mouse button in the centre of the red frame and drag the frame to the desired position.

6.8.2.2 Motion detection window

The Motion window appears when Motion Detection is active. It displays the configured motion detection threshold level. The amount of motion currently being detected is shown as a blue graph line relative to the motion detection threshold level.



The configured motion detection threshold level



Peaks rising above the set motion detection level will trigger an alarm and possibly actions as well.

Motion Detection alarms will not trigger if the Motion Detection function is disabled or while the Motion Detection settings are saving. In these cases, the motion indication window displays the text, Motion Detection Is Not Active.

Motion detection is disabled.

6.8.3 Network failure detection

System > Events > Network failure detection

Ping request

The network failure detection function enables the CD/(I)FD820 to test the connection between the camera and a target host on the network. The camera can ping the remote machine - that is, send data packets to it, with configurable intervals to determine if it is accessible and responding. Appropriate actions can be selected to be triggered if the ping request times out without a response. Being capable of implementing local recording when network failure occurs, the camera can be a backup recording device for the surveillance system.

Detection Switch

Click *On* or *Off* to enable or disable the Network failure detection alarm, respectively. Alternatively, you can click *By schedule* to select a schedule that you have configured through the *Schedule* page.

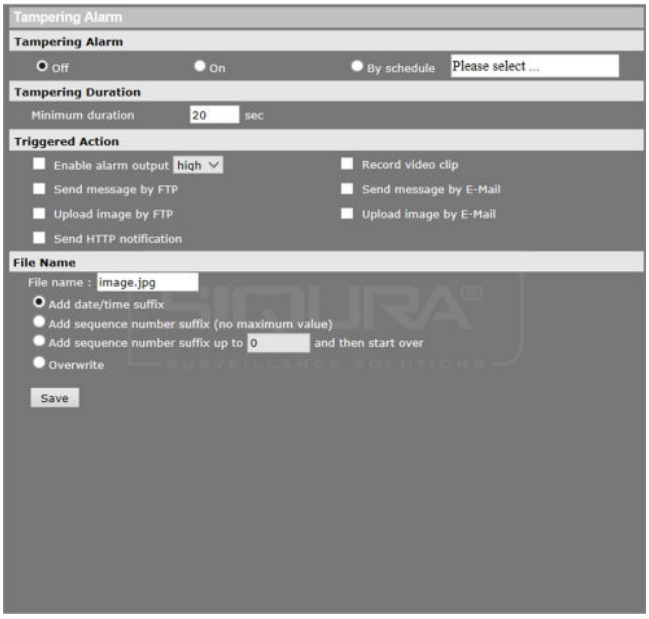
Detection Type

The IP address you specify here will be pinged at the interval entered for "every *n* minutes". The range is from 1 to 99 minutes.

Triggered Action

Select the desired trigger actions which are to be performed in the event of an alarm. For more information, see *Triggered Action*.

6.8.4 Tampering



System > Events > Tampering

On the Tampering page, administrators can enable the camera to trigger an alarm when changes to the physical state of the camera occur. The Tampering Alarm enables the camera to detect tampering actions - deliberate redirection of the camera, blocking, paint spraying, and lens covering - through video analysis and react to such events by sending out notifications or uploading snapshots to the specified destination(s).

Detection of camera tampering is achieved by measuring the differences between older frames of video (which are stored in buffers) and more recent frames.

To enable the Tampering alarm

1 On the *System* tab, click **Tampering** in the menu on the left.

2 Under *Tampering Alarm*, select **On**.

The default setting is *Off*.

Alternatively, you can click *By schedule* to select a schedule that you have configured through the *Schedule* page.

3 Under *Tampering Duration*, enter a *Minimum Duration* of video analysis to determine whether tampering has occurred.

The longer the minimum duration, the higher the tampering threshold. The Tampering Duration range is from 10 to 3600 seconds. Default: 20 seconds.

4 Under *Triggered Action*, select the actions to be performed on the occurrence of a tampering alarm. For more information, see *Triggered Action*.

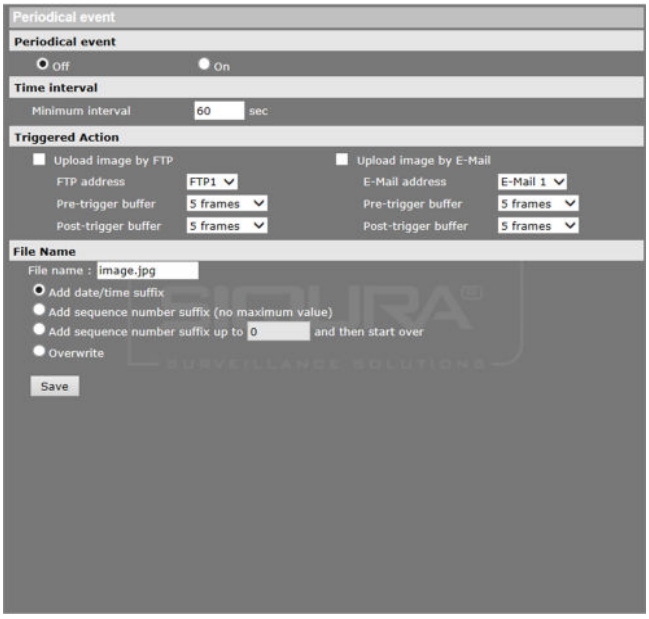
5 If applicable, under *File name*, specify a file name for a file to be sent when an alarm occurs, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.

6 Click **Save**.

SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions.

Important: Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

6.8.5 Periodical event



System > Events > Periodical event

On the Periodical event page, users can set the camera to upload images periodically to an FTP site or an email address. For example, if the time interval is set to 60 seconds, the camera will upload images to the assigned FTP site or email address every 60 seconds. The images to be uploaded are the images before and after the triggered moment. In the Triggered Action section users can define how many images are to be uploaded.

Periodical event

The default setting for the Periodical Event function is *Off*. Enable the function by selecting *On*.

Time interval

The default value of the time interval is 60 seconds. The setting range of the time interval is from 60 to 3600 seconds

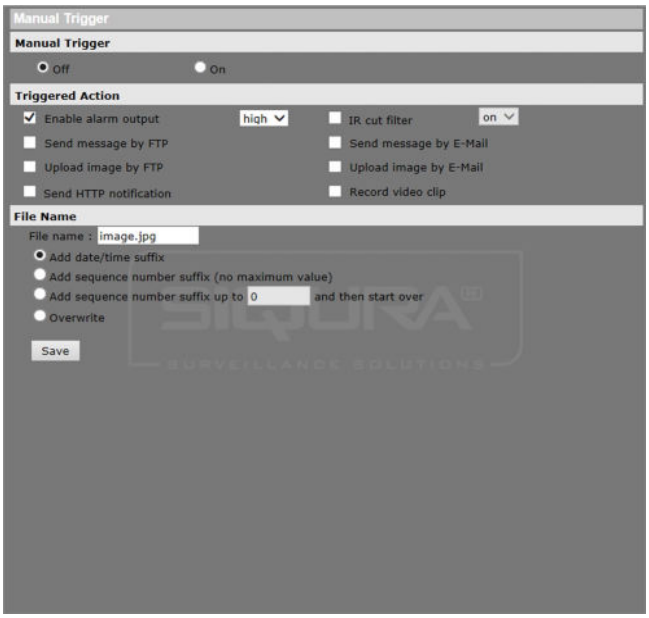
Triggered action

Select the desired trigger actions which are to be performed in the event of an alarm. For more information, see the *Triggered Action* section.

File name

The File name text box allows users to specify the file name conventions for captured images. For more information, see *Specifying file name conventions*.

6.8.6 Manual trigger



System > Events > Manual trigger

Using the Manual Trigger function, the current image(s) or video can be uploaded to the appointed destination, such as an FTP site or an email address. The administrator can specify the actions to be performed when the user clicks the Manual Trigger button on the Home page.

Manual Trigger

Click *On* or *Off* to enable or disable the Manual Trigger function, respectively.

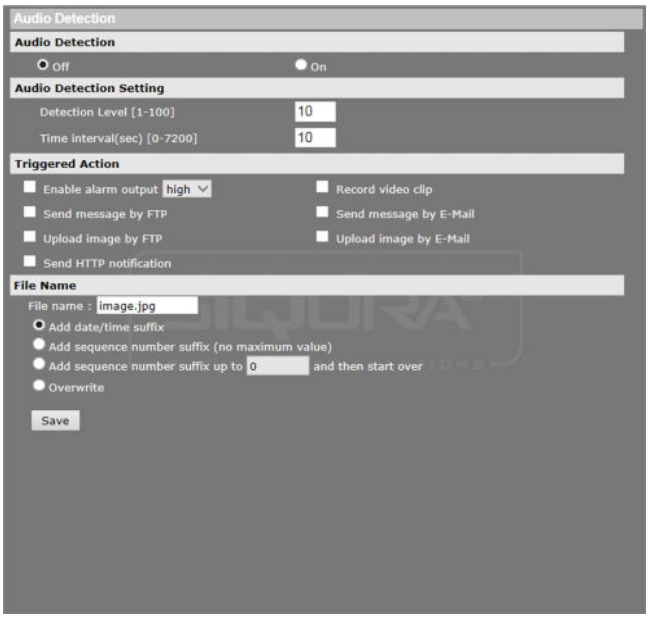
Triggered Action

Select the desired trigger actions which are to be performed in the event of an alarm. For more information, see the *Triggered Action* section.

File name

The File Name text box allows users to specify the file name conventions for captured images. For more information, see *Specifying file name conventions*.

6.8.7 Audio detection



System > Events > Audio detection

The Audio detection function allows the camera to detect audio and trigger alarms when the audio volume in the detected area reaches/exceeds the determined sensitivity threshold value.

To enable Audio detection

1. On the *System* tab, click **Events** in the menu on the left.
2. Click **Audio detection**.
3. Under *Audio Detection,* select **On**.

   The default setting is *Off*.
4. Under *Audio Detection Setting*, type a *Detection Level* value.

   This value sets the detection level for each sampling volume; the smaller the value, the more sensitive it is. The default level is 10.
5. Under *Audio Detection Setting*, type a *Time interval* value.

   The value is the interval between each detected audio event. The default interval is 10.
6. Under *Triggered Action*, select the actions to be performed when audio is detected. For more information, see the *Triggered Action* section.
7. If applicable, under *File name*, specify a file name for a file to be sent when audio is detected, and then select an option to add a suffix to the file name or overwrite the previous file. For more information, see *Specifying file name conventions*.
8. Click **Save**.

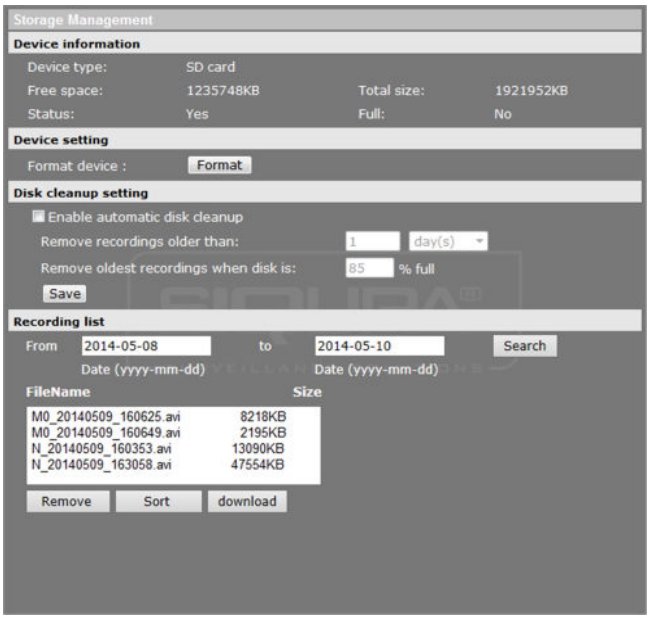
   SMTP, FTP, and/or HTTP configuration must be completed prior to using these protocols in alarm actions.

Important: Uploading images by FTP or e-mail is only possible if MJPEG output is configured. If only H.264 streaming is enabled, no images will be sent.

6.9 Storage management

Recorded video can be stored on a microSD card inserted into the camera or on a network share.

6.9.1 SD Card



System > Storage management > SD Card

You can implement local recording using a microSD/SDHC card up to 64 GB. On the Storage Management page, administrators can view capacity information of the microSD/SDHC card and a recording list with all the recording files that are saved on the memory card. Administrators can also format the SD card and implement automatic recording cleanup.

Note: Format the microSD/SDHC card when using it for the first time. Formatting is also required when a memory card already used on one camera is transferred to another camera with a different software platform.

To implement and activate recording to the SD card

- On the *Storage Management* page, format the card, if necessary, and configure disk cleanup settings.
- On the *Recording* page, set a recording schedule.

  - and/or -
- Under *Triggered action* on the *Application*, *Motion detection, Network failure detection*, *Tampering*, *Manual trigger*, or *Audio detection* webpage, select **Record video clip**.

  When the recording mode is set to *Always* (consecutive recording) and microSD/SDHC card recording is also allowed to be triggered by events, the system will immediately start recording to the memory card once events occur. The camera will return to the regular recording mode when event recording stops.

Device information

The Device information section of the Storage Management page shows:

- The type of storage card
- The amount of free space available on the card
- The total amount of storage on the card
- Status - whether or not there is a card in the microSD slot of the camera
- Full - whether or not the card has any available memory

Device setting

Under Device setting, the administrator can format or reformat an inserted SD card.

Warning: Formatting the SD card erases *all* information on the card. Be sure to download any information on the card you want to save before reformatting. See *Recording list* below for more information.

Disk cleanup setting

Use this section to remove old recordings automatically. You can set it to remove recordings older than the specified number of days or weeks and/or to remove recordings starting with the oldest on the card when a specified percentage of the card is full.

Recording list

Each video file on the microSD/SDHC card is listed in the Recording list. The maximum file size is 60 MB per file. When the recording mode is set to "Always" (consecutive recording) and the microSD/SDHC card recording is also allowed to be triggered by events, the system will immediately start event recording to the memory card when an event occurs. The camera returns to the regular recording mode after event recording stops.

Using the *From/To* time boxes, users can search the recorded files in a specified time range. Two file formats - that is, *.avi (video format) and *.jpeg (image format), are available for selection. The following capital letters are used to indicate the recording type:

- A: Alarm
- M: Motion detection
- N: Network failure
- R: Regular (scheduled recording)
- T: Tampering
- U: Audio detection

Files can be removed, sorted, and downloaded.

To remove a file

1. Click on the selected file.
2. Press the **Remove** button.
   The file is deleted from the card.

To sort the files by name and date

- Click **Sort**.

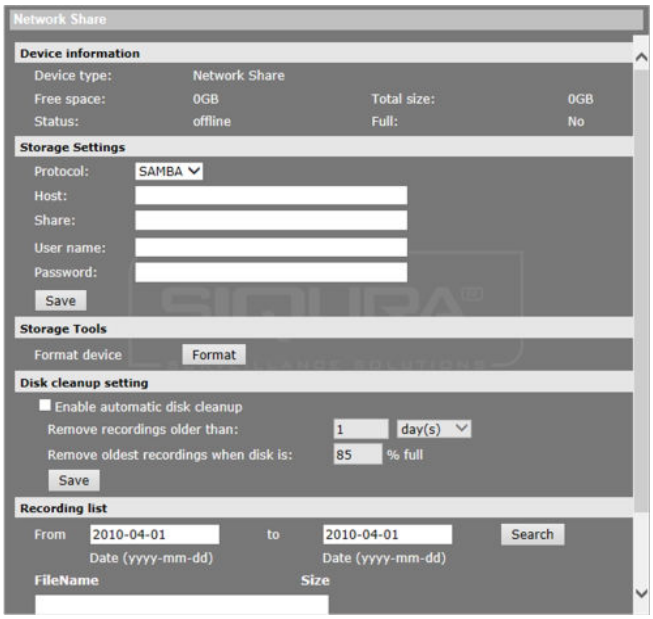
To save or view a recording file

1. In the Recording list, select a file.
2. Click **Download**.

A window appears with a link to the file.

3 Click on the link to save the file locally or to play it in your default viewing software.

6.9.2 Network Share



System > Storage management > Network Share

The CD/(I)FD820 supports recording video to a network share. On the Network Share page, administrators can view capacity information of the network share and a recording list with all the recording files that are saved on the network share. Administrators can also format the network share and implement automatic recording cleanup.

To implement and activate recording to the network share

1 On the *Network Share* page, use the *Host* and *Share* boxes in the *Storage Settings* section to specify the path to the network share.

2 In the *User name* and *Password* boxes, provide the credentials required to access the network share.

3 Click **Save**.

The network share status information appears in the Device information section.

4 Format the network share, if necessary, and configure disk cleanup settings.

> **Warning:** Formatting the network share erases *all* information on the share. Be sure save a copy of any information on the share you need to keep before reformatting. See *Recording list* below for more information.

5 On the *Recording* page, set a recording schedule.

- and/or -

Under *Triggered action* on the *Application*, *Motion detection, Network failure detection*, *Tampering*, *Manual trigger*, or *Audio detection* webpage, select **Record video clip**.

When the recording mode is set to *Always* (consecutive recording) and recording is also allowed to be triggered by events, the system will immediately start recording to the network share once events occur. The camera will return to the regular recording mode when event recording stops.

Device information

The Device information section of the Network Share page shows:

- The type of storage device
- The amount of free space available on the device
- The total amount of storage on the device
- Status - whether the device is offline or online

Full - whether or not there is storage space available

Storage Settings

Use this section to provide details regarding the protocol to be used, the path to the network share, and the user's identity. If you cannot access the network share, verify that the network settings are correctly configured and that you have the required share and user permissions.

Format device

Clicking *Format* erases all information on the network share.

Disk cleanup setting

Use this section to remove old recordings automatically. You can set it to remove recordings older than the specified number of days or weeks and/or to remove recordings starting with the oldest on the disk when a specified percentage of the disk is full.

Recording list

Each video file on the network storage card is listed in the Recording list. The maximum file size is 60 MB per file. When the recording mode is set to "Always" (consecutive recording) and recording to network storage is also allowed to be triggered by events, the system will immediately start event recording to the network storage when an event occurs. The camera returns to the regular recording mode after event recording stops.

Using the *From/To* time boxes, users can search the recorded files in a specified time range. Two file formats - that is, *.avi (video format) and *.jpeg (image format), are available for selection. The following capital letters are used to indicate the recording type:

- A: Alarm
- M: Motion detection
- N: Network failure
- R: Regular (scheduled recording)
- T: Tampering
- U: Audio detection

Files can be removed, sorted, and downloaded.

To remove a file

1 Click on the selected file.
2 Press the **Remove** button.
The file is deleted from the network storage.

To sort the files by name and date

- Click **Sort**.

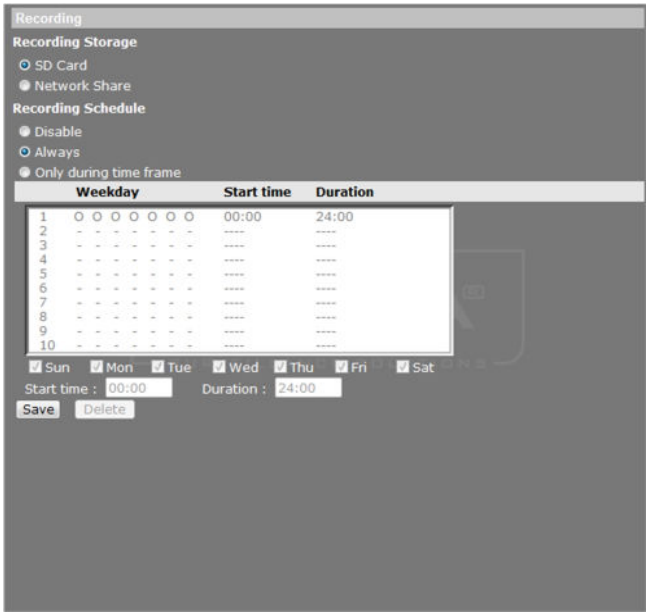
To save or view a recording file

1 In the Recording list, select a file.
2 Click **Download**.

A window appears with a link to the file.

3 Click on the link to save the file locally or to play it in your default viewing software.

6.10 Recording


Recording
Recording Storage
SD Card
Network Share
Recording Schedule
Disable
Always
Only during time frame
Weekday
Start time
Duration
1 O O O O O O O 00:00 24:00
2 - - - - - - - ----- -----
3 - - - - - - - ----- -----
4 - - - - - - - ----- -----
5 - - - - - - - ----- -----
6 - - - - - - - ----- -----
7 - - - - - - - ----- -----
8 - - - - - - - ----- -----
9 - - - - - - - ----- -----
10 - - - - - - - ----- -----
Sun Mon Tue Wed Thu Fri Sat
Start time : 00:00
Duration : 24:00
Save
Delete

System > Recording

Recording schedules

Administrators can configure up to 10 recording schedules that meet the surveillance requirements. Recordings are stored on the microSD/SDHC card or on a network share.

- Select **Disable** to terminate the recording function - that is, if no scheduled recording is desired.
- Select **Always** for continuous recording.

To configure a recording schedule for a specific time frame

1 On the *System* tab, click **Recording** in the menu on the left.

2 Under *Recording Storage*, click **SD Card** or **Network Share**.

3 Select **Only during time frame**.

4 On the schedule overview, click on the row (1-10) representing the schedule you wish to configure.

5 To add days to the schedule, select the appropriate check boxes.

6 Specify the start time and duration of the recording.

Duration range: 0 to 168 hours.

7 Click **Save**.

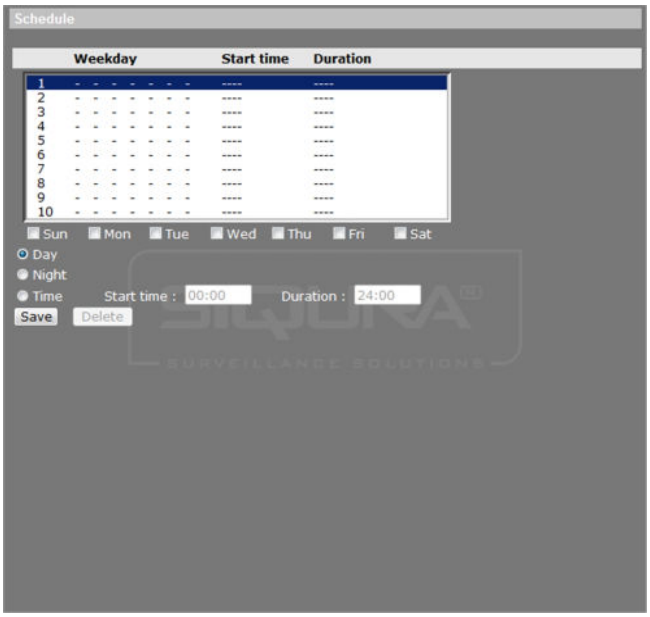
To delete a recording schedule

1 On the schedule overview, select the schedule that you want to delete.

2 Click **Delete**.

For information, see also *SD Card* and *Network Share*.

6.11 Schedule


Schedule
Weekday
Start time
Duration
1 - - - - - - - ---- ----
2 - - - - - - - ---- ----
3 - - - - - - - ---- ----
4 - - - - - - - ---- ----
5 - - - - - - - ---- ----
6 - - - - - - - ---- ----
7 - - - - - - - ---- ----
8 - - - - - - - ---- ----
9 - - - - - - - ---- ----
10 - - - - - - - ---- ----
Sun Mon Tue Wed Thu Fri Sat
Day
Night
Time
Start time : 00:00
Duration : 24:00
Save
Delete

System > Schedule

On the Schedule page, Administrators can create up to ten time schedules that meet the surveillance requirements for functions, such as Motion detection, Application, and Network failure detection.

To create a schedule

1. On the *System* tab, click **Schedule** in the menu on the left.
2. On the schedule overview, click on the row (1-10) representing the schedule that you wish to configure.
3. To add days to the schedule, select the appropriate check boxes.
4. To specify the start time and duration of the schedule, click either **Day** or **Night**, or click **Time**, and then set the start time and duration.

   Duration range: 00:00 to 168:59
5. Click **Save**.

To delete a schedule

1. On the schedule overview, select the schedule that you want to delete.
2. Click **Delete**.

Note: You need to select **By Schedule** on pages such as Motion detection and Network failure detection to enable the Schedule function.

6.12 File location

System > File location

The CD/(I)FD820 offers JPEG snapshot and MJPEG recording functionality. Users can specify a storage location for the snapshots and live video recordings. The default storage location is `C:\`.

Note: For users with a Windows 7 operating system, it is required to log on as an Administrator to configure the Snapshot and Web Recording function.

To change the storage location:

1 Enter the new location in the *All files stored at:* box.

Note: Make sure the selected file path contains only valid characters such as letters and numbers.

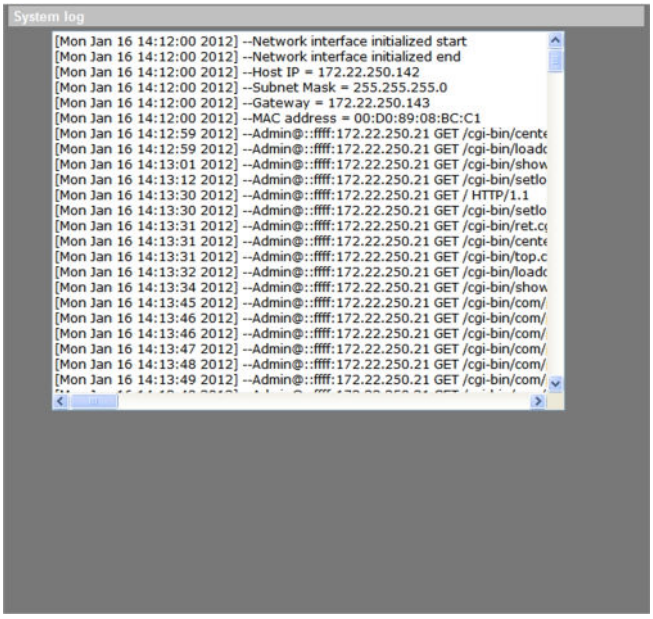
2 Alternatively, click **Select** to browse for a location.

3 Once you have chosen a new location, click **Save**.
All new snapshots and recorded video will be saved to the designated location.

6.13 View information

Via the *View information* option in the left-hand pane, administrators can access the camera log file, display user information, and get an overview of the camera parameters and their current values.

6.13.1 Log file


System log
[Mon Jan 16 14:12:00 2012] --Network interface initialized start
[Mon Jan 16 14:12:00 2012] --Network interface initialized end
[Mon Jan 16 14:12:00 2012] --Host IP = 172.22.250.142
[Mon Jan 16 14:12:00 2012] --Subnet Mask = 255.255.255.0
[Mon Jan 16 14:12:00 2012] --Gateway = 172.22.250.143
[Mon Jan 16 14:12:00 2012] --MAC address = 00:D0:89:08:BC:C1
[Mon Jan 16 14:12:59 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/cente
[Mon Jan 16 14:12:59 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/loadc
[Mon Jan 16 14:13:01 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/show
[Mon Jan 16 14:13:12 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/setlo
[Mon Jan 16 14:13:30 2012] --Admin@::ffff:172.22.250.21 GET / HTTP/1.1
[Mon Jan 16 14:13:30 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/setlo
[Mon Jan 16 14:13:31 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/ret.c
[Mon Jan 16 14:13:31 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/cente
[Mon Jan 16 14:13:31 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/top.c
[Mon Jan 16 14:13:32 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/loadc
[Mon Jan 16 14:13:34 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/show
[Mon Jan 16 14:13:45 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/com/
[Mon Jan 16 14:13:46 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/com/
[Mon Jan 16 14:13:46 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/com/
[Mon Jan 16 14:13:47 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/com/
[Mon Jan 16 14:13:48 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/com/
[Mon Jan 16 14:13:49 2012] --Admin@::ffff:172.22.250.21 GET /cgi-bin/com/

System > View information > Log file

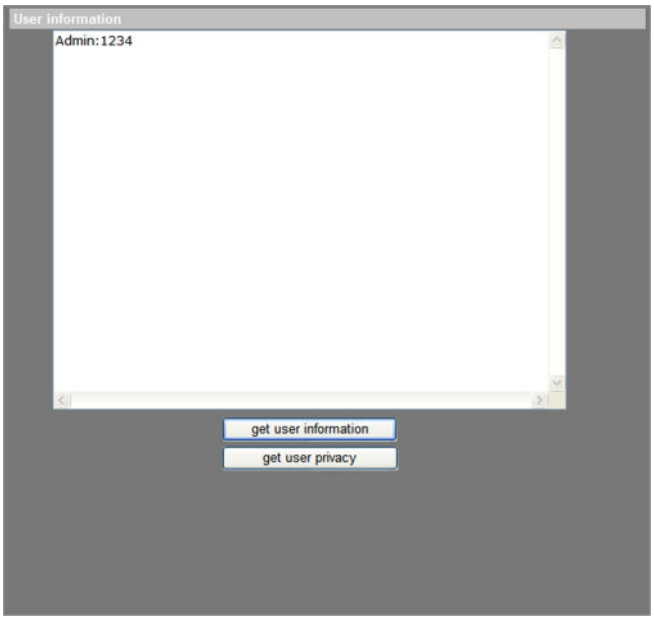
The system log provides useful information about the configuration and connections after system launch.

To view the system log

- On the *System* tab, click **View information** in the menu on the left, and then click **Log file**.

  The system log is displayed.

6.13.2 User Information



System > View information > User information

The Administrator can view each added user's login information and privileges. See also *User*.

To view the list of user accounts

- On the *System* tab, click **View information** in the menu on the left, and then click **User information**.

  A list of users and their passwords displays.

  "Viewer: 4321" indicates that the login name is "Viewer", and the password is "4321".

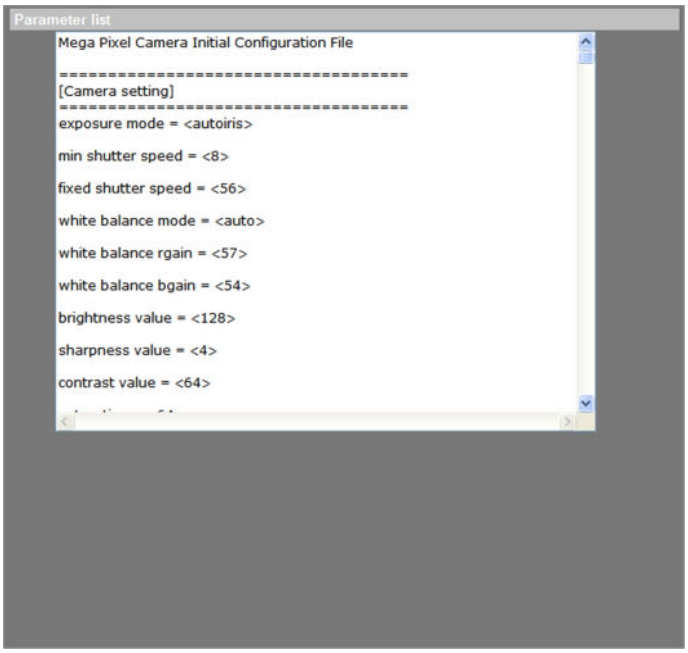
To view the user permissions

1. On the *System* tab, click **View information** in the menu on the left, and then click **User information**.
2. Click **Get User Privacy**.

   A list of users and their privileges displays.

   Each of the four numbers after every user name corresponds to one of the four permissions in the following order: I/O access, Camera control, Talk, and Listen. The number 1 indicates that a privilege is granted; the number 0 indicates that a privilege is denied. For more information, see *User*.

6.13.3 Parameters



System > View information > Parameters

The CD/(I)FD820 camera's parameters are stored in its configuration file.

To view the system parameters

- On the *System* tab, click **View information** on the menu on the left, and then click **Parameters**.

  The parameters display in the browser.

Note: Refresh the webpage to view the most current parameter values.

6.14 Factory default

Factory default
Restore factory settings and lose any changes?
System will restart and need installer program to setup network.
Full Restore
Restore factory settings (excluding network settings)
Partial Restore
Reboot the system.
Reboot

System > Factory default

The Factory default page enables administrators to reset the camera to the default factory settings.

To perform a full restore to the default factory settings

1 On the *System* tab, click **Factory default** in the menu on the left.

2 Click **Full Restore**.

The system will restart in 30 seconds.

> **Note:** The camera's IP address will be restored to the factory default IP address - that is, 10.x.x.x.

To perform a partial restore (excluding the network settings)

1 On the *System* tab, click **Factory default** in the menu on the left.

2 Click **Partial Restore**.

The system will restart in 30 seconds.

> **Note:** The camera's current network settings will not be affected by the restore.

To restart the system without changing its settings

- Click **Reboot**.

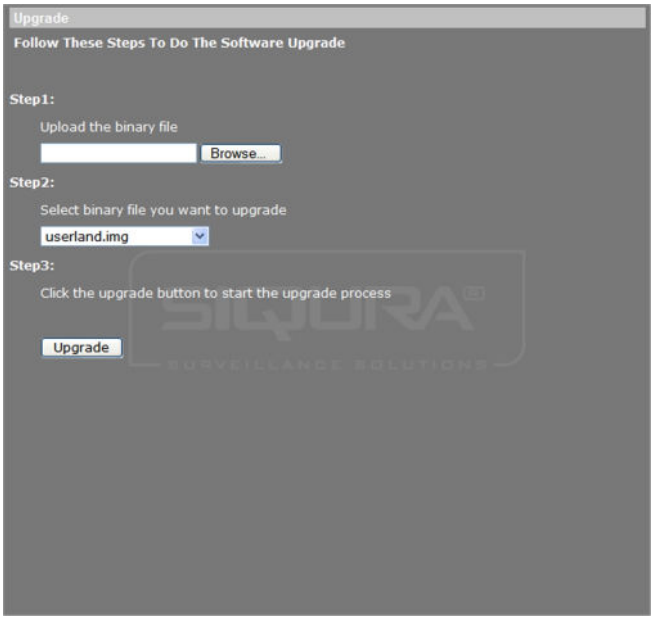
6.15 Software version

System > Software version

To display the camera's software version

- On the *System* tab, click **Software version** in the menu on the left.
  Version information displays in the web browser. Note that version numbers appearing in your web page may differ from the numbers shown in the example above.

6.16 Software upgrade



System > Software upgrade

Administrators can upgrade the software of the CD/(I)FD820 on the Software upgrade page.

Important: Upgrading the software also resets the factory default settings, including the IP address. Make sure to note all settings before proceeding.

To upgrade the software of your camera

1 Make sure that the upgrade software file is available before attempting to upgrade software.

2 On the *System* tab, click **Software upgrade** in the menu on the left.

3 Click **Browse** and select the location and binary file to be uploaded, such as `userland.img`, for example.

Note: Software upgrade file names must be `userland.img`. Other file upgrades should only be performed by qualified technicians. Do not change the upgrade file name, or the system will fail to find the file.

4 Select the file to be upgraded from the *Select binary file you want to upgrade* list.

5 Click **Upgrade**.

The upgrade process starts. Progress is shown by an upgrade status bar.

When the upgrade process is complete, the web browser returns to the home page and operation can continue.

6 Close your web browser.

7 On the Windows **Start Menu**, click **Control Panel**, and then click **Programs and Features**.

8 In the programs list, select **Siqura Viewer**, and then click **Remove** to uninstall the existing Siqura Viewer.

9 Reopen your web browser, log on to the CD/(I)FD820, and then allow the automatic download and installation of Siqura Viewer.

6.17 Maintenance

System > Maintenance

Administrators can use this page to export configuration files (`.bin`) to a specified location for future use.

To export the configuration file

1 On the *System* tab, click **Maintenance** in the menu on the left.
2 Press **Export**.
3 In the *File Download* dialog box, select **Open** or **Save**.
4 If saving the file, choose the local directory where it should be saved.

It is also possible to upload an existing configuration file to the camera.

To upload a configuration file

1 On the *System* tab, click **Maintenance** in the left column.
2 To locate the required file, click **Browse**.
3 When you have selected the desired file, click **Upload**.

7 Streaming

On the Streaming tab, Administrators can adjust settings related to video format, video compression, the Region of Interest (ROI), video text overlay, video stream protocol, video frame rate, video masking, and audio transmission mode.

In This Chapter

7.1 Video format..... 70

7.2 Video compression..... 72

7.3 Video ROI..... 73

7.4 Video text overlay..... 74

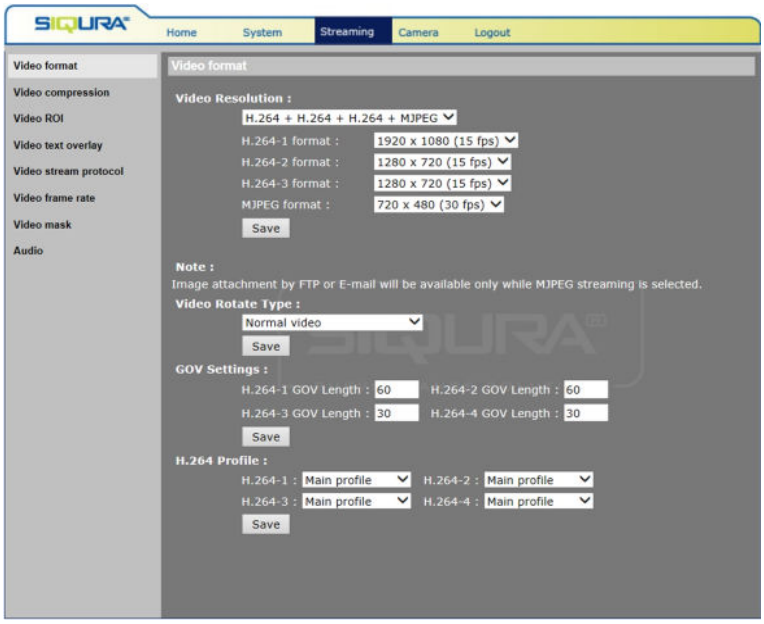
7.5 Video stream protocol..... 75

7.6 Video frame rate..... 76

7.7 Video mask..... 77

7.8 Audio..... 78

7.1 Video format



Streaming tab

On the Video format page, users can adjust settings related to video resolution, image orientation, GOV length, and per stream they can select an H.264 profile.

7.1.1 Video resolution

To set up the video resolution for the CD/(I)FD820

1 On the *Streaming* tab, click **Video format** in the menu on the left.
2 On the **Video Resolution** list, select a streaming format combination.
3 Using the video format list(s), select the preferred resolution setting(s).
4 Click **Save** to confirm the setting.

Note: Image attachment by FTP or e-mail is available only when MJPEG streaming is selected.

7.1.2 Video rotate type

A camera can be oriented in a variety of ways for different applications.

To select a video rotation type

1 On the *Streaming* tab, click **Video format** in the menu on the left.
2 Choose one of the following video rotation types:
- **Normal video.** The camera's orientation is not modified.
- **Flip video.** The image rotates across the horizontal axis.
- **Mirror video.** The image rotates across the vertical axis.
- **90 degree clockwise.** The image rotates 90° clockwise.
- **180 degree rotate.** The image rotates 180°.
- **90 degree counterclockwise.** The image rotates 90° counterclockwise.

3 Click **Save** to confirm settings.

7.1.3 GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. Less bandwidth is needed if the GOV length is set to a high value. However, the shorter the GOV length the better the video quality is.

To configure the GOV settings

1 On the *Streaming* tab, click **Video format** in the menu on the left.
2 In the *GOV Settings* section, type the values in the GOV Length boxes.
Range: 2 to 64.
The default value for H.264-1 / H.264-2 / H.264-3 / H.264-4 is 60 / 60 / 30 / 30 (NTSC) or 50 / 50 / 25 / 25 (PAL).
3 Click **Save** to confirm the GOV setting.

7.1.4 H.264 Profile

Users can set each H.264 profile to Baseline Profile, Main Profile, or High Profile according to the compression needs. The default setting is Main Profile.

To set an H.264 profile

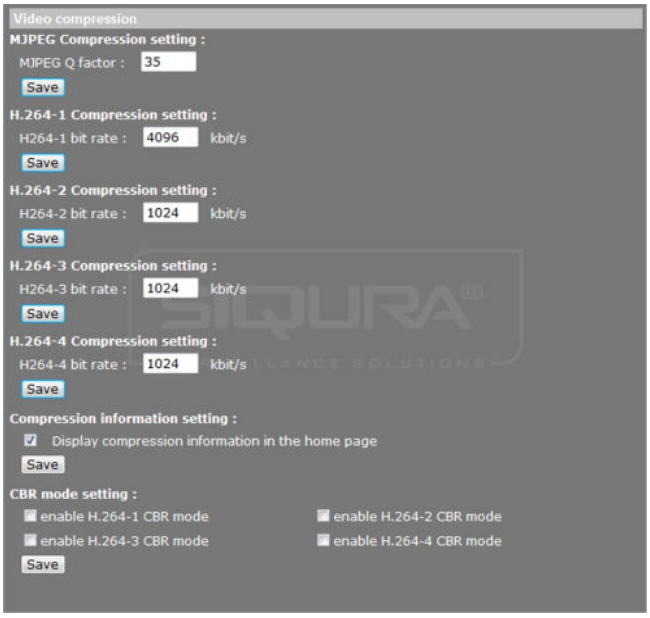
1 On the *Streaming* tab, click **Video format** in the menu on the left.

2 In the **H.264-x** list, select the desired profile.
Options: Baseline profile, Main profile, High profile.

Note: Make sure that the profile you select is supported by the system.

3 Click **Save**.

7.2 Video compression



Streaming > Video compression

Administrators can select the appropriate video compression mode for an application on the Video compression page.

To change MJPEG compression settings

1 On the *Streaming* tab, click **Video compression** in the menu on the left.
2 Set a value for the *MPEG Q factor* parameter.
Range: [1...70]. Default setting: 35. Higher values give higher image quality. They require higher bit rates, though, and therefore consume more bandwidth.
3 Click **Save** to confirm settings.

To change H.264 compression settings

1 On the *Streaming* tab, click **Video compression** in the menu on the left.
2 Set values for the bit rates for each H.264 video stream.
Range H.264-1: [64...8192] kbps. Default: 4096 kbps.
Range H.264-2: [64...2048] kbps. Default: 1024 kbps.
Range H.264-3: [64...2048] kbps. Default: 1024 kbps.
Range H.264-4: [64...2048] kbps. Default: 1024 kbps.
3 Click **Save** to confirm settings.

To display compression information on the home page

1 On the *Streaming* tab, click **Video compression** in the menu on the left.

2 Select the **Display compression information in the home page** check box.

3 Click **Save** to confirm settings.

To enable constant bit rate (CBR) mode

Constant bit rate (CBR) mode may be preferred if the available bandwidth is limited. It is important to take the image quality into account when choosing a CBR mode.

1 On the *Streaming* tab, click **Video Compression** in the menu on the left.

2 Click to select CBR mode for the applicable H.264 video stream(s).

3 Click **Save**.

7.3 Video ROI

Streaming > Video ROI

ROI stands for Region of Interest. This function allows users to select a specific monitoring region for 2nd, 3rd and 4th streams, instead of showing the full image.

Note: This function is only available when triple streams or higher is selected under Video Resolution on the Video format page.

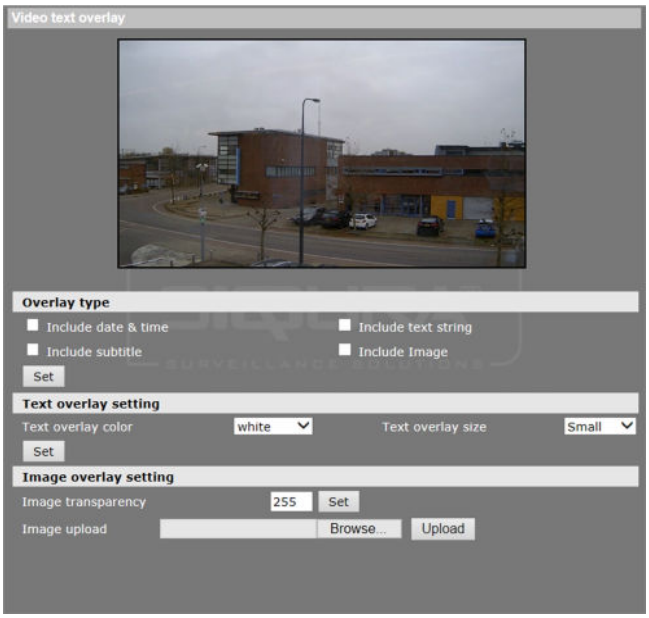
To set the ROI for a stream

1 Click the check box of the stream for which you want to set a ROI.
The red ROI frame is displayed.

2 Drag the frame to move it to the desired position.

3 Drag the edges or corners of the frame to resize it.

7.4 Video text overlay



Streaming > Video text overlay

The CD/(I)FD820 features programmable on-screen display (OSD) facilities. Date and time information, a subtitle, a text string, and an image (such as a logo) can be displayed as overlays over the camera images.

To add a text overlay

1 On the *Streaming* tab, click **Video text overlay** in the menu on the left.
2 Click to select the overlay type(s) you wish to add.
Include date & time: available options are 'date', 'time', or 'date & time'.
Include subtitle: up to three text boxes can be used.
Include text string: type the text you wish to add; maximum length: 20 alphanumeric characters.
3 Align the text(s) as necessary and drag the text box(es) to the desired position on the preview.
4 Click **Set**.
5 In the **Text overlay color** list, select a font colour.
6 In the **Text overlay size** list, set the text size to small, medium or large.
7 Click **Set**.

To add an image overlay

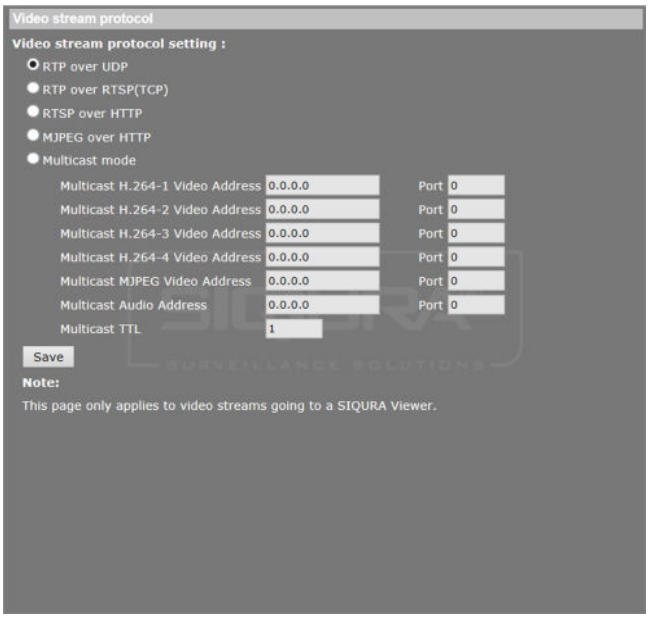
1 On the *Streaming* tab, click **Video text overlay** in the menu on the left.
2 In the *Overlay type* section, click **Include Image**.
3 Drag the image box to the desired position on the preview.
4 Under *Image overlay setting*, click **Browse.**
5 Locate and select an image that meets the following requirements:
- Format: 8-bit .bmp
- Width: a multiple of 32 pixels
- Height: a multiple of 4 pixels
6 Click **Upload**.

7 Type a value in the *Image transparency* box.
Range: 0 - 255.

8 Click **Set**.

Camera view with three overlays: Image overlay (top left), Date & time (bottom left), and Text string (bottom right)

7.5 Video stream protocol


Video stream protocol
Video stream protocol setting :
RTP over UDP
RTP over RTSP(TCP)
RTSP over HTTP
MJPEG over HTTP
Multicast mode
Multicast H.264-1 Video Address 0.0.0.0 Port 0
Multicast H.264-2 Video Address 0.0.0.0 Port 0
Multicast H.264-3 Video Address 0.0.0.0 Port 0
Multicast H.264-4 Video Address 0.0.0.0 Port 0
Multicast MJPEG Video Address 0.0.0.0 Port 0
Multicast Audio Address 0.0.0.0 Port 0
Multicast TTL 1
Save
Note:
This page only applies to video streams going to a SIQURA Viewer.

Streaming > Video stream protocol

On the Video Stream Protocol page, users can select a protocol for streaming media over the network to the webpages via the Siqura Viewer application.

Protocol	Description
RTP over UDP	Real-Time Transport Protocol, using UDP transport, lessens network delay and is required for two-way audio streams.
RTP over RTSP (TCP)	Real-Time Transport Protocol, using TCP transport, guarantees that data is delivered and that no packets are dropped, but some network delay may occur.
RTSP over HTTP	A standard solution to help RTSP work through firewalls and Web proxies, so that viewers behind a firewall can access RTSP streams.
MJPEG over HTTP	Consecutive JPEG images are sent individually over HTTP.
Multicast mode	Multicast streaming reduces bandwidth usage for streams being transmitted to multiple clients.

To set a video stream protocol

1 On the *Streaming* tab, click **Video stream protocol** in the menu on the left.

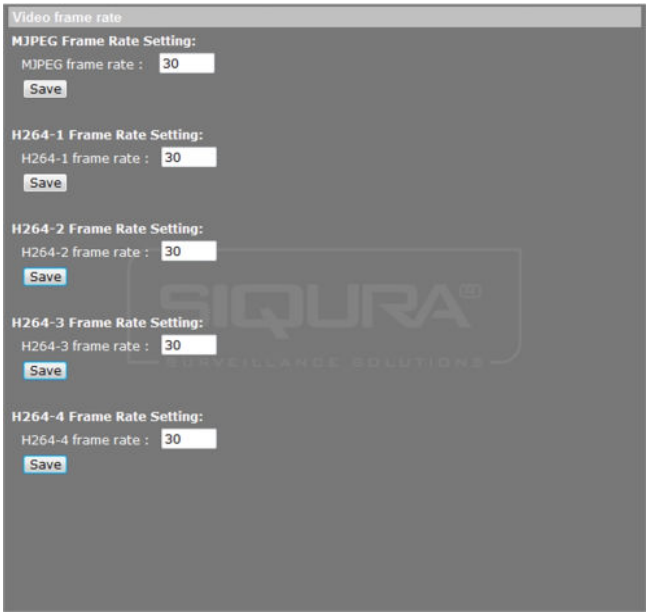
2 Select a streaming protocol.

To use Multicast mode, you must also supply the Multicast IP address and the appropriate video and audio ports. In the Multicast TTL text box, specify the number of routers (hops) that multicast traffic is permitted to pass before expiring on the network

3 Click **Save**.

Note: Only RTP over UDP supports two-way audio.

7.6 Video frame rate

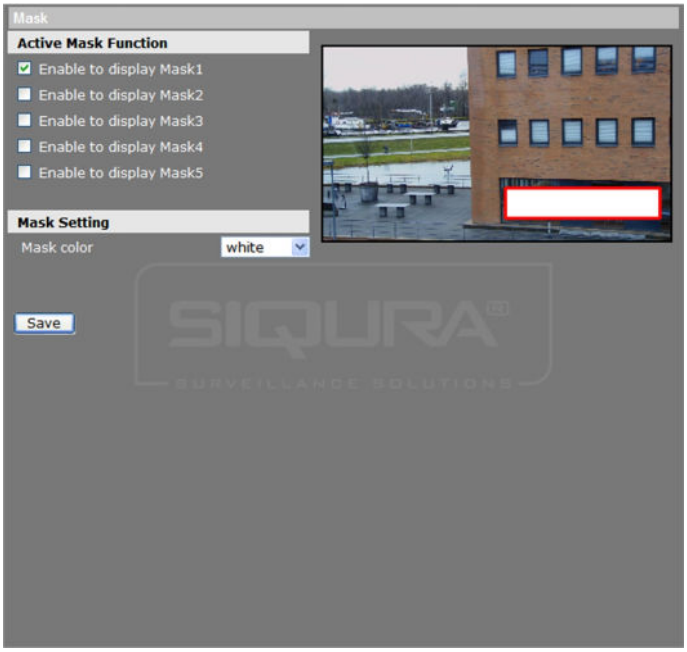


Streaming > Video frame rate

On the Video frame rate page, the administrator can set the MJPEG, H.264-1, H.264-2, H.264-3, and H.264-4 frame rate - that is, the number of frames per second. The default frame rate is 30 fps. The setting range is from 1 to 30 fps. After setting a value, click **Save** to confirm your setting.

Note: Lower frame rates will decrease video smoothness.

7.7 Video mask



Streaming > Video mask

The video mask function aims to avoid any intrusive monitoring. The CD/(I)FD820 supports up to five privacy masks.

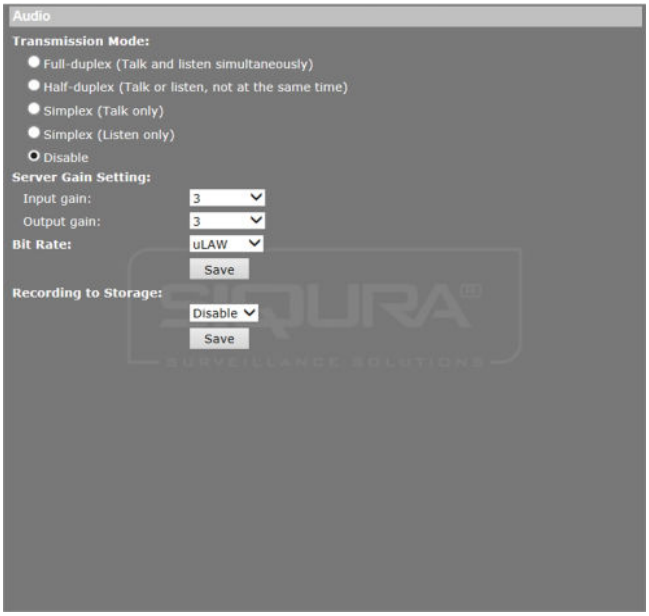
To add a mask

1 On the *Streaming* tab, click **Video mask** in the menu on the left.
2 Under *Active Mask Function*, select a mask check box.
A red frame overlay is superimposed over the camera view on the right.
3 Use your pointer to adjust the size of the mask and position it on the target zone.
4 Under *Mask Setting*, select a fill colour.
5 Click **Save**.
The fill colour you selected is applied to the mask.

To remove a mask

1 On the *Streaming* tab, click **Video mask** in the menu on the left.
2 Under *Active Mask Function*, clear the check box of the mask you wish to remove.
3 Click **Save**.
The mask is removed.

7.8 Audio



Streaming > Audio

On the Audio page, administrators can select the transmission mode and bit rate for audio streams.

To configure audio settings

1 On the *Streaming* tab, click **Audio** in the menu on the left.

2 Under *Transmission Mode*, click to select one of the following options:

- **Full-duplex** – Audio can be transmitted and received at the same time, so local and remote sites can communicate with each other simultaneously.
- **Half-duplex** – Audio can be either transmitted or received, so one site can talk or listen to the other site in turn.
- **Simplex (Talk only)** – Audio can be transmitted, so one site can speak to the other site.
- **Simplex (Listen only)** – Audio can be received, so one site can listen to the other site.
- **Disable** – The audio transmission function is turned off.

3 Under *Server Gain Setting*, select audio input/output gain levels for sound amplification.

Audio gain values are adjustable from 1 to 6. Set the audio gain to **Mute** to turn off the sound.

4 On the *Bit Rate* list, select the audio transmission bit rate.

Audio transmission bit rates include the following options:

- 16 kbps (G.726)
- 24 kbps (G.726)
- 32 kbps (G.726)
- 40 kbps (G.726)
- μ-LAW (64 kbps) (G.711)
- A-LAW (64 kbps) (G.711)

Both μ-LAW and A-LAW imply 64 kbps. However, μ-LAW and A-LAW use different compression formats.

While higher bit rates allow for better audio quality, they also require more bandwidth.

5 Click **Save**.

Note: CD820 series cameras support Audio in only.

To enable audio recording

1 Under *Recording to Storage*, click **Enable** if you wish to add audio when recording video to the SD card or network share.

2 Click **Save**.

8 Camera

From the Camera tab, Administrators and users with the camera control permission can view a live video stream and configure camera parameters.

Note: After making changes in any section in the pane on the left, click the SET button to confirm the new settings and see the effect of your changes in the camera view.

In This Chapter

8.1 Exposure..... 80

8.2 White Balance..... 82

8.3 Picture Adjustment.....83

8.4 Backlight..... 84

8.5 Digital Zoom..... 84

8.6 IR Function (FD820 & IFD820).....84

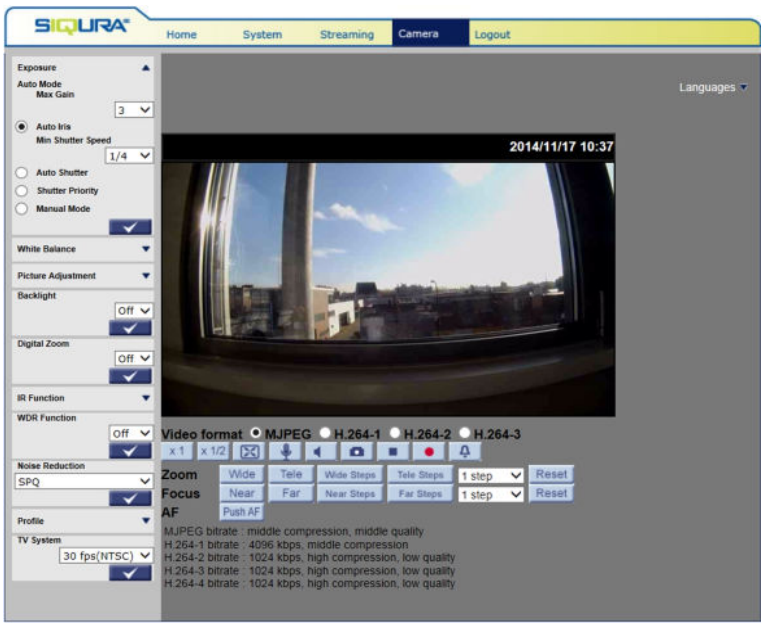
8.7 WDR Function.....85

8.8 Noise Reduction.....85

8.9 Profile..... 86

8.10 TV System..... 87

8.1 Exposure



Camera > Exposure (FD820)

Exposure is the amount of light received by the image sensor and is determined by the width of iris adjustment (lens diaphragm), the amount of exposure by the sensor (shutter speed), and other exposure parameters. The CD/(I)FD820 features both automatic and manual exposure adjustment.

8.1.1 Auto mode

Max Gain

Maximum Gain can be set to reduce image noise. Max Gain range is 1 dB to 3 dB. Select *Off* to disable the function. Default setting: 3 dB.

Auto Iris (fixed focal lens excluded)

In this mode, the camera automatically shuts the iris to suit the environment illumination. The minimum shutter speed can be set from 1/30 to 1 sec (NTSC) or 1/25 to 1/1.5 sec (PAL). AGC (Auto Gain Control) will function automatically according to the light conditions of the subject.

Auto Shutter

This function controls the shutter speed and adjusts the iris automatically according to the light intensity. It is also effective if a fixed iris lens is being used. The minimum shutter speed range is configurable from 1/500 to 1 sec (NTSC) or 1/425 to 1/1.5 sec (PAL).

Shutter Priority

In this mode, it is the shutter speed that takes main control of the exposure. Shutter speed can be set to values ranging from 1/500 to 1/30 sec (NTSC) or 1/425 to 1/25 sec (PAL).

Note: This mode is not available for fixed focal length models.

8.1.2 Manual mode

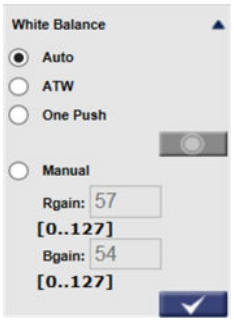
Shutter speed

In this mode, users can select the suitable shutter speed and gain value according to the environmental illumination. The shutter speed range is from 1/10000 to 1 sec (NTSC) or from 1/10000 to 1/1.5 sec (PAL).

Gain

The gain value range is from 1 dB to 9 dB, or select *Off* to disable the function.

8.2 White Balance



Camera > White Balance

A camera needs to measure the quality of a light source and create a reference colour temperature in order to calculate all the other colours. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance control modes, according to the operating environment. The table below provides the colour temperatu res of some light sources as a general reference.

Light source	Colour temperature in °K
Cloudy sky	6000 to 8000
Noon sun and clear sky	6500
Household lighting	2500 to 3000
75 watt bulb	2820
Candle flame	1200 to 1500

Auto

The camera detects a colour temperature range and calculates an optimal white balance. The Auto White Balance mode is suitable for light sources with colour temperature ranges from 2700 to 7800 K.

ATW

In Auto Tracking White Balance (ATW) mode, the camera continuously adjusts the colour balance to changes in the colour temperature which may occur, for example, when moving from an indoor scene to an outdoor scene. The ATW mode is suitable for environments with light sources ranging from 2500 K to 10000 K.

One Push

With the One Push function, white balance is adjusted and fixed according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. The function is suitable for light sources with any kind of colour temperature.

To set the white balance using One Push

1 Point the camera at the area to be monitored.
2 Under *White balance*, click **One Push**.
3 Click the **Set** button.
The Trigger button is activated.
4 Click the **Trigger** button to adjust the white balance.
White Balance is adjusted.

The Trigger button remains active.

Note: In this mode, the value of white balance will not change as the scene or the light source varies. Therefore, users may have to re-adjust the white balance by pushing the Trigger button again when needed.

Manual

In this mode, users can change the white balance value manually by adjusting the Rgain and Bgain (red and blue). Rgain/Bgain values range from 0 to 127.

8.3 Picture Adjustment

Camera > Picture Adjustment

Brightness

Users can set the brightness of the image by selecting a value ranging from -12 to +13. To increase video brightness, select a higher number.

Sharpness

The sharpness value controls the clarity of detail perceived in an image. A higher sharpness value may enhance the edges of objects and produce a clearer image. A lower sharpness value can result in a more obscure image. The sharpness value is adjustable from 0 to 15.

Contrast

The contrast setting controls the differences in colour and light which make an object distinguishable from other objects or its background. Camera image contrast levels range from -6 to +19.

Saturation

The saturation setting controls the intensity of the colour in an image. Saturation can be set on a scale of -6 to +19.

Hue

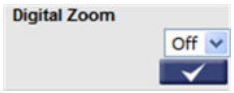
The hue setting controls the actual colour of the pixels of the image. Hue can be set on a scale of -12 to +13.

8.4 Backlight

Camera > Backlight

Backlight Compensation (BLC) enhances the visibility of objects in the foreground of an image when there is a bright light in the background.

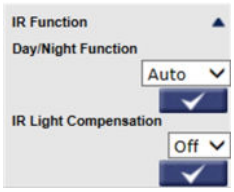
8.5 Digital Zoom



Camera > Digital Zoom

If digital zoom is enabled, users can rotate the mouse wheel in full screen mode to zoom in and out. Digital zoom is adjustable from x2 to x8.

8.6 IR Function (FD820 & IFD820)



Camera > IR Function

Day/Night Function

With the IR cut filter, the camera can still catch clear images at night or in low-light conditions.In daylight, the IR cut filter blocks infrared light for clear images; at night, the IR cut filter is removed to utilise infrared light and the displayed images will be in black and white.

Auto

The camera decides the occasion to remove the IR cut filter.

Night

The camera removes the IR-cut filter and switches to monochrome.

Day

The IR cut filter is returned and the image is in colour.

Smart

Smart mode enhances the monochrome/night mode stability in the scenario that IR illumination is dominant. In this mode, when the IR illuminator is turned on, the IR cut filter of the IP camera will keep open (i.e. monochrome/night mode), preventing the camera from returning to the colour/day mode when IR illumination is dominant.

Models with IR LEDs

Cameras with built-in IR LED module have three additional IR function modes:

- Light sensor mode: the IR LEDs are controlled by the light sensor
- Light on mode: IR LED lights are always on
- Light off mode: IR LED lights are always off

IR Light compensation

Automatic IR light compensation at night.

8.7 WDR Function

Camera > WDR Function

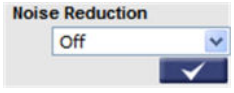
WDR function

The wide dynamic range (WDR) function automatically adjusts settings and varies the exposure for different objects in the camera scene in order to display detail in the darker areas of an image without saturation in the brighter parts. WDR is especially effective in solving indoor and outdoor contrast issues. The user can enable or disable the WDR function, according to the application.

Scale

WDR is adjustable from *Low*, *Mid*, to *Hi*. A higher level of WDR represents wider dynamic range, so that he IP camera can catch a greater scale of brightness.

8.8 Noise Reduction



Camera > Noise Reduction

The CD/(I)FD820 provides multiple noise reduction options for delivering optimised image quality especially in extra low-light conditions.

3DNR

Level options for 3D Noise Reduction (3DNR) include *Low*, *Mid,* and *High*. A higher level of 3DNR generates relatively enhanced noise reduction.

SPQ

The proprietary Smart Picture Quality (SPQ) video processing method can drastically minimise motion blur and reduce noise especially in low-light environments. The combination of SPQ and 3DNR at different levels further yields exceptional video performance in various conditions.

8.9 Profile

Camera > Profile

Combinations of settings made on the Camera tab can be stored as profiles which can be used for specific scenarios.

To create a profile

1 On the *Camera* tab, configure the various camera settings as needed.
2 Open the **Profile** section.
3 Click the **Num** list, and then select a number for the profile.
4 Type the profile name in the *Name* box.
5 Click **Set**.
6 To link the profile to a schedule you have configured on the *Schedule* page, select **By schedule**.
7 Click the **Schedule** box, and then select a schedule.
Multiple schedules can be selected.
8 Click **Set**.

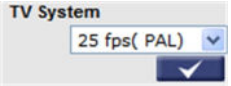
To activate a profile

1 On the *Camera* tab, click to open the **Profile** section.
2 In the **Num** list, select the required number.
3 Click the **Activate** button.
The camera adopts the settings associated with the profile.

To delete a profile

1 On the *Camera* tab, click to open the **Profile** section.
2 In the **Num** list, select the profile to be deleted.
3 Click in the **Name** box, and then click the Close button which pops up.
4 Click **Set**.

8.10 TV System



Camera > TV System

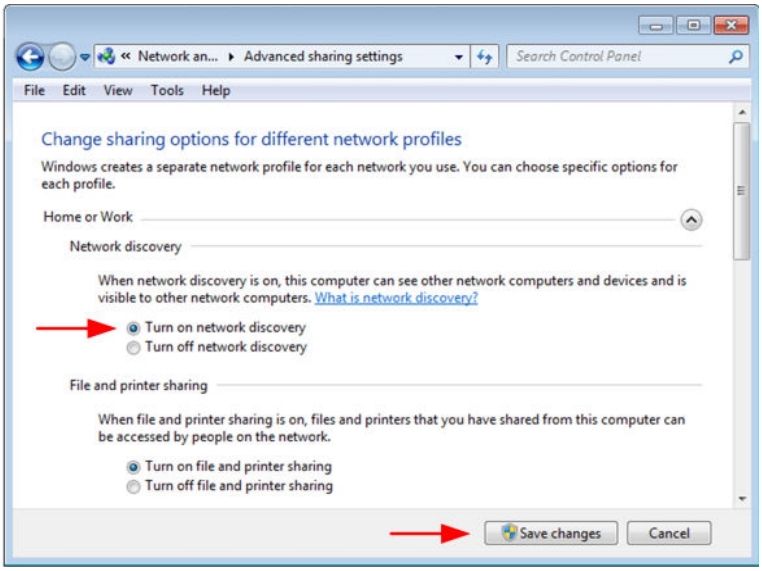
Select the video format that matches the TV system (either NTSC or PAL) associated with the camera.

Appendix: Enable UPnP components in Windows 7

With UPnP enabled in Windows, it is possible to see Siqura devices in Windows Explorer. You can double-click a device to open its webpages.

To enable UPnP in Windows 7

1 In *Control Panel*, click **Network and Sharing Center**.
2 In the left pane, click **Change advanced sharing settings**.
3 Under the relevant network profile, click **Turn on network discovery**.
4 Click **Save changes**
UPnP will now automatically start when you turn on your computer.


« Network an... ▸ Advanced sharing settings
Search Control Panel
File Edit View Tools Help
Change sharing options for different network profiles
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.
Home or Work
Network discovery
When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?
Turn on network discovery
Turn off network discovery
File and printer sharing
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.
Turn on file and printer sharing
Turn off file and printer sharing
Save changes
Cancel

Enable network discovery

Appendix: Delete the existing Siqura Viewer software

Viewing camera images in the CD/(I)FD820 webpages requires Siqura Viewer software. We strongly advise you to remove a previous installation of Siqura Viewer from your computer before you access the camera over the network for the first time or when you encounter an "A new version is available" message.

To uninstall Siqura Viewer

1. On the Windows **Start Menu**, click **Control Panel**.
2. Click **Programs and Features**.
3. On the *Uninstall or change a program* page, select **Siqura Viewer** from the list of installed programs.
4. Click **Uninstall**.

Deleting the files in your Temporary Internet Files folder may improve your web browser performance.

To delete the Temporary Internet files

1. Open your web browser.
2. On the **Tools** menu, click **Internet Options**.
3. In the *Browsing history* section of the *General* tab, click **Delete**.
4. Select **Temporary Internet files**, and then click **Delete**.

Appendix: Set up Internet security

If ActiveX control (Siqura Viewer) installation is blocked, set the Internet security level to default or change the ActiveX controls and plug-ins settings.

To set the Internet Security level to default

1 Start Internet Explorer (IE).
2 On the **Tools** menu, select **Internet Options**.
3 Click the **Security** tab, and then select the (logo of the) **Internet** zone.
4 Under *Security level for this zone*, click the **Default Level** button.
5 Click **OK** to confirm the setting.
6 Close the browser window, and start a new session to access the CD/(I)FD820.

To modify ActiveX Controls and Plug-ins settings

1 Start Internet Explorer (IE).
2 On the **Tools** menu, select **Internet Options**.
3 Click the **Security** tab, and then select the (logo of the) **Internet** zone.
4 Under *Security level for this zone*, click the **Custom Level** button.
The Security Settings - Internet Zone dialog box displays.
5 Under *ActiveX controls and plug-ins*, set all items listed below to **Enable** or **Prompt**.
Note that items may vary from one IE version to another.

- Allow previously unused ActiveX controls to run without prompt.
- Allow Scriptlets.
- Automatic prompting for ActiveX controls.
- Binary and script behaviors.
- Display video and animation on a webpage that does not use external media player.
- Download signed ActiveX controls.
- Download unsigned ActiveX controls.
- Initialize and script ActiveX controls not marked as safe for scripting.
- Run ActiveX controls and plug-ins.
- Script ActiveX controls marked safe for scripting.

6 Click **OK** to accept the settings and close the *Security Settings* dialog box.
7 Click **OK** to close the Internet Options dialog box.
8 Close the browser window, and start a new session to access the CD/(I)FD820.

Index

A

About this manual..... 6
Access the webpages..... 14
Acquire an IP address automatically..... 33
Add and manage user accounts..... 27
Admin password..... 27
Advanced settings..... 35
Appendix: Delete the existing Siqura Viewer software..... 89
Appendix: Enable UPnP components in Windows 7..... 88
Appendix: Set up Internet security..... 90
Application..... 44
Audio..... 78
Audio detection..... 55
Auto mode..... 81

B

Backlight..... 84
Basic..... 33

C

CA certificate..... 32
Camera..... 80
Cautions..... 9
CD820/IFD820..... 20
Change the network settings with Siqura Device Manager..... 16
Client certificate and private key..... 32
Compliance..... 10
Connect via web browser..... 14
Create a self-signed certificate..... 30
Create and install a signed certificate..... 30

D

Daylight saving time..... 25
DDNS..... 40
Description..... 13
Digital Zoom..... 84

E

Events..... 43
Exposure..... 80

F

Factory default..... 66
FD820..... 21
File location..... 62
Find the unit with Siqura Device Manager... 15
FTP..... 42

G

GOV Settings..... 71

H

H.264 Profile..... 71
Home..... 20
Home page functions..... 22
Host name..... 25
HTTP..... 43
HTTPS..... 29

I

IEEE 802.1X..... 32
Install Siqura Viewer..... 18
IP filter..... 31
IPv6 address configuration..... 35
IR Function (FD820 & IFD820)..... 84

L

Log file..... 63
Log on to the unit..... 17

M

Mail..... 41
Maintenance..... 68
Manual mode..... 81
Manual trigger..... 54
Models..... 11
Modify the fixed IP address..... 34
Motion detection..... 48
Motion detection area..... 49
Motion detection window..... 50

N

Network..... 33
Network failure detection..... 51
Network Share..... 58
Noise Reduction..... 85

P

Parameters..... 65
Periodical event..... 53
Picture Adjustment..... 83
Product overview..... 11
Profile..... 86

Q

QoS..... 36

R

Recording..... 60

S

Safety.....7
Safety and compliance..... 7
Schedule..... 61
SD Card..... 56
Security..... 26
SNMP.....37
Software upgrade..... 67
Software version..... 67
Specifying file name conventions..... 47
Storage management.....56
Streaming..... 70
Streaming Authentication Setting.....28
System..... 25
System requirements..... 14
System settings.....24

T

Tampering..... 52
The CD/(I)FD820 Web Interface..... 18
Time format.....26
Time synchronisation..... 26
Time zone..... 25
Triggered action..... 45
TV System.....87

U

UPnP.....39
Use PPPoE..... 35
User..... 27
User Information..... 64

V

Video compression.....72
Video format.....70
Video frame rate..... 76
Video mask.....77
Video resolution..... 71
Video ROI.....73
Video rotate type.....71
Video stream protocol..... 75
Video text overlay.....74
View information..... 62

W

WDR Function..... 85
White Balance..... 82

Z

Zoom and focus (FD820)..... 23